Tampereen yliopisto

Riikka Tanner

# SUOMEN KYBERTURVALLISUUSSTRATEGIA JA TIEDUSTELULAKIUUDISTUS

## Turvallisuusongelmia vai turvallistamisongelmia?

Johtamisen ja talouden tiedekunta
Pro gradu -tutkielma
Helmikuu 2019

# TIIVISTELMÄ

RIIKKA TANNER: SUOMEN KYBERTURVALLISUUSSTRATEGIA JA TIEDUSTELULAKIUUDISTUS:
Turvallisuusongelmia vai turvallistamisongelmia?
Pro gradu -tutkielma
Tampereen yliopisto
Politiikan tutkimuksen tutkinto-ohjelma
Helmikuu 2019

---

Tällä hetkellä maailmanpolitiikkaa, yhteiskuntaa ja yrityksiä voimakkaimmin ravisteleva muutosvoima liittyy analogisen maailman digitaaliseen murrokseen. Samalla kun käsityksemme todellisuudesta muuttuu muuttuneen toimintaympäristön myötä, muuttuu myös käsityksemme turvallisuudesta. Kyberturvallisuudesta on tullut uusi turvallisuuden ulottuvuus.

Tähänastinen kyberturvallisuuden tutkimus on ollut suhteellisen vähäistä mitä selittää osaltaan se, että ilmiönä ja käsitteenä kyberturvallisuus on saavuttanut jalansijaa vasta viimeisen vuosikymmenen aikana. Monet perinteiset kansainvälisen politiikan teoriakoulukunnat ovat laiminlyöneet kyberturvallisuuden tutkimuksen tai rinnastaneet sen perinteiseen turvallisuudentutkimukseen.

Tämä tutkimus pyrkii ymmärtämään kyberturvallisuutta ilmiönä ja sitä miten ilmiö näyttäytyy erityisesti turvallistamisen kontekstissa. Tutkimuksen teoreettisena tukijalkana toimii Kööpenhaminalainen koulukunta, jonka perusajatuksia ja teorioita esitellään muun muassa puheaktiteorian kautta. Tutkimuksen kannalta olennaisena teoriana toimii turvallistamisen teoria ja Juha A. Vuoren turvallistamisen prosessin vaiheistus ja tyypittely. Aineiston läpikäyntiin, joka koostuu sekä viranomaislähteistä, että Helsingin Sanomien ja Ylen uutisartikkeleista, on sovellettu kriittistä diskurssianalyysiä.

Tutkimuksen keskiössä on tapaustutkimus Suomen tiedustelulainsäädännön uudistamisesta. Tutkimuskohteena on Suomen kyberturvallisuusstrategia ja sen osana esimerkkitapauksena siviilitiedustelulainsäädännön eli tiedustelulain valmisteluun vuosina 2015-2018 liittyvä poliittinen keskustelu. Tarkoituksena on selittää ja selvittää sitä, millainen turvallistamisen prosessi Suomessa on kyberturvallisuuteen liittyen käynnissä ja millaisin diskurssein ja puheaktein turvallistamista tapahtuu.

Turvallistamisen prosessi nähdään tyypillisesti janana, jonka toisessa päässä on epäpoliittisena pidetyt asiat, keskivaiheilla selvästi politisoituneet julkisessa keskustelussa olevat asiat ja toisessa ääripäässä turvallistetut asiat, jotka ovat jo poliittisen keskustelun ulkopuolella.

Tutkimus osoittaa selvästi, miten turvallistamisen mekanismit toimivat kyberturvallisuus -keskustelun ympärillä ja miten tiedustelulainsäädännön uudistus on siirtänyt painopisteen turvallistamisen janalla kohti turvallistettua lopputulosta. Tutkimuksen aineistosta nousee selkeästi esiin viitteitä useasta eri turvallistamisen tyypistä, mitkä tukevat sitä lopputulosta, että kyberturvallisuuden turvallistamista on tapahtunut vuodesta 2013 lähtien.

Avainsanat: Kyberturvallisuus, tiedustelulaki, turvallistaminen

# SISÄLLYSLUETTELO

# 1. JOHDANTO

Tällä hetkellä maailmanpolitiikkaa, yhteiskuntaa ja yrityksiä voimakkaimmin ravisteleva muutosvoima liittyy analogisen maailman digitaaliseen murrokseen. Maailma ja sen myötä toimintaympäristömme on muuttunut fyysisen lisäksi digitaaliseksi ykkösten ja nollien muodostamiksi bittiketjuiksi. Digitalisaatiota voidaan kuvata dynaamiseksi tiedon ja viestinnän evoluutioksi, missä teknologia mahdollistaa uudenlaisten ratkaisujen ja toimintamallien syntymisen koko ajan nopeutuvalla vauhdilla. Ihmisten lisäksi koneet ja esineet kytkeytyvät globaaliin virtuaaliseen ympäristöön muodostaen ”kaiken internetin” (Internet of Everything), jossa tieto liikkuu saumattomasti ja nopeasti eri rajapintoja hyödyntämällä luoden samalla uudenlaisia verkostoja. [1] Ennusteiden mukaan verkkojen välillä liikkuva tietomäärä kaksinkertaistuu kahden vuoden välein, mikäli nykyinen kehitysvauhti jatkuu.[2]

Samalla kun käsityksemme todellisuudesta muuttuu muuttuneen toimintaympäristön myötä, muuttuu myös käsityksemme turvallisuudesta. Rikollisuus, aktivismi ja jopa sodat ovat siirtyneet verkkoon samaa tahtia kuin internetin ja teknologian kehitys ovat sen mahdollistaneet. Tätä digitaalisen ajan turvallisuutta kuvaamaan käytetään termiä *kyberturvallisuus.* Tämän kyberturvallisuuden puolustajina valtioilla on erityinen rooli. Samalla kun tietoisuus yhteiskunnan riippuvuudesta tietoverkkoihin on lisääntynyt, on alettu kiinnittää entistä enemmän huomiota myös verkon nurjaan puoleen ja niihin uhkiin, mitä lisääntynyt riippuvuus tietoverkoista aiheuttaa.[3]

Tästä riippuvuussuhteesta johtuen kyberturvallisuus on ennen kaikkea tasapainon hakemista uhkien mutta myös kybermaailman meille tarjoamien mahdollisuuksien välillä.[4] Digitalisaation ennenkokematon vauhti on saanut myös suuret turvallisuuspoliittiset toimijat kuten valtiot heräämään uuteen todellisuuteen. Muun muassa Yhdysvallat on määritellyt jo vuodesta 2013 lähtien kyberuhkat merkittävimmäksi uhkaksi omalle kansalliselle turvallisuudelleen. Myös Suomi on vastannut digitalisaation haasteeseen julkaisemalla oman kyberturvallisuusstrategiansa (2013), mikä muodostaa myös osan tämän tutkimuksen

[1] Limnéll et al. 2014, 18-19.
[2] mt. 2014, 18.
[3] mt. 2014, 20-21.
[4] mt. 2014, 15.

keskeisestä aineistosta. Valtioiden ja turvallisuustoimijoiden näkökulman siirtyminen analogisesta turvallisuudesta digitaaliseen onkin ennen kaikkea strateginen muutos.[5]

Myös kansainvälisen politiikan tutkimuksen on pysyttävä muutoksen perässä. Alan vakiintuneita teorioita ja malleja on testattava yhä uudelleen ja sovellettava uusiin käyttötapauksiin. Jos maailma muuttuu, eikö meidän tutkijoina tule muuttua sen mukana? Kybertoimintaympäristön ja sen turvallisuuden merkitys kasvaa nopeasti mutta monella tapaa akateeminen tutkimus ei ole pysynyt muutoksen vauhdissa mukana. Tämä asettaa myös poliittiselle päätöksenteolle haasteita. Jos emme ymmärrä riittävästi ilmiöstä ympärillämme, miten voimme luottaa siihen että näitä asioita koskeva päätöksenteko perustuu riittävään analyysiin ja todellisuuteen? Oma näkökulmani on, että vaikeista, monimutkaisistakin asioista pitää pystyä tuottamaan tutkimuksellista aineistoa ymmärrettävässä muodossa julkisen keskustelun tueksi - tiedettä tai tutkimusta ei tehdä vain akateemikoita ja toisia tutkijoita varten. Silloin kun halutaan tehdä tutkimusta, jota on tieteenalan ulkopuoleltakin mahdollista ymmärtää, korostuu empirian merkitys. Tapaustutkimus sopii tällaiseen tutkimuksen tekemiseen erinomaisesti. Konkreettista tapausta selittämällä meidän on helpompi ymmärtää sitä laajempaa ilmiötä.

Historia kirjoittaa itse itseään ja ilmiöt saattavat olla olemassa vain hetken aikaa ennen kuin muuttuvat osaksi historiaa. Tutkimus tarkastelee aina kohdettaan hyvin rajatussa kontekstissa, tiettynä ajanhetkenä, tietyn asian tai ilmiön representaationa. Tämä tutkimus asemoi itsensä osaksi kansainvälisen politiikan tutkimusta keskittymällä kyberturvallisuudentutkimukseen ja osaksi sosiaalisen konstruktivismin perinnettä hyödyntämällä kriittistä diskurssianalyysiä ja siihen pohjautuvaa puheaktiteoriaa aineiston analysointivaiheessa. Tutkimusaihetta, -asetelmaa ja näihin liittyviä valintoja läpikäydään tarkemmin seuraavassa luvussa.

Luku kolme pureutuu tarkemmin siihen, mikä tutkimuksen tieteenfilosofinen lähtökohta on ja mistä löytyvät kyberturvallisuustutkimuksen juuret. Teoreettista viitekehystä esitellään lähtemällä liikkeelle turvallisuuden- ja kyberturvallisuuden käsitteistä ja siitä miten kokemuksemme turvallisuudesta ylipäätään syntyy. Tämä johdattelee meidät kohti turvallisuuden tutkimusta osana kansainvälisen politiikan tutkimusta ja sitä, miten kansainvälisen politiikan eri koulukunnat ovat perinteisesti lähestyneet ja suhtautuneet kyberturvallisuuden tutkimukseen.

[5] Limnéll et al. 2014, 21.

Tutkimuksen teoreettisena tukijalkana toimii Kööpenhaminalainen koulukunta, jonka perusajatuksia ja teorioita esitellään muun muassa puheaktiteorian kautta. Tutuiksi tulevat myös tämän tutkimuksen kannalta olennaisena teoriana turvallistamisen teoria ja turvallistamisen prosessin eri vaiheet ja tyypit.

Tähänastinen kyberturvallisuuden tutkimus on ollut suhteellisen vähäistä mitä selittää osaltaan se, että ilmiönä ja käsitteenä kyberturvallisuus on saavuttanut jalansijaa vasta viimeisen kymmenen vuoden aikana. Monet perinteiset kansainvälisen politiikan teoriakoulukunnat ovat laiminlyöneet kyberturvallisuuden tutkimuksen tai rinnastaneet sen perinteiseen turvallisuudentutkimukseen. Keskeiset kyberturvallisuuden ja turvallistamisen yhteyttä tarkastelleet tutkimukset, kuten Barry Buzanin sekä Lene Hansenin ja Helen Nissenbaumin näkökulmat nostetaan esiin tämän tutkimuksen teoriaosuudessa, luvuissa 3.1 ja 3.2. Vaikka monet turvallisuuden tutkimuksen peruselementit pätevät myös kyberturvallisuuteen, liittyy siihen myös sellaisia elementtejä, joita perinteisten teorioiden on vaikea selittää. Vähintäänkin meidän tulee olla tietoisia siitä miten kyberturvallisuusympäristö muovautuu ja rakentaa itseään, pyrkien samalla säilyttämään näkyvyys tässä ympäristössä vaikuttaviin toimijoihin.

Konstruktivismi luokin tälle tutkielmalle luontevan perusteoreettisen viitekehyksen ja lähestymistavan tutkimusmetodiikkaan. Käsitteenä kyberturvallisuus läpileikkaa yhteiskuntatieteen, taloustieteen ja informaatiotieteen rajat, mistä syystä on luonnollista valita konstruktivismi tutkimuksen lähtökohdaksi sen salliessa empiirisen vapauden[6] soveltaa tutkielmaan soveltuvia teorioita ja konsepteja ja metodeja myös edellä mainituilta tieteenaloilta.[7]

Tämän tutkimuksen keskiössä on tapaustutkimus Suomen tiedustelulainsäädännön uudistamisesta. Tapaus kuvaa hyvin kyberturvallisuusilmiötä ja siihen liittyvää keskustelua laajempana kokonaisuutena. Laadullinen tutkimus on kuitenkin aina tiettyyn kontekstiin tai aikaan sidottua tutkimusta. Varsinkin tiedustelulain tapauksessa on huomioitavaa, että lainsäädännön valmistelu on edelleen kesken. Lopputulos ei siis ole vielä selvillä, vaikkakin helmikuuhun 2019 mennessä meillä on hyvä käsitys siitä, mikä lain lopputulos tulee olemaan. Todellisuus muovautuu sitä mukaa kuin sitä elämme. Siinä piileekin konstruktivistisen ajattelun

[6] Eriksson et al. 2007, 19.
[7] Tuomi et al. 2009, 55.

voima. Lopputuloksia ja johtopäätöksiä tämän hetken ja tämän tutkimuksen kontekstissa tarkastellaan luvussa viisi.

Olen kiinnostunut tästä aiheesta sekä ammatillisessa mielessä, että yksityisenä kansalaisena, jota tuleva tiedustelulainsäädännön uudistus koskettaa. Olen yli kymmenen vuoden ajan työskennellyt IT -sektorilla ja nähnyt omakohtaisesti teknologian ottamat valtavat kehitysaskeleet ja sen, millaisia haasteita tämä asettaa alan eri toimijoille. IT – alalla työskenteleville tietoturva ja kyberturvallisuuteen liittyvät uhkakuvat ovat läsnä joka päivä.

Pyrkimyksenä on myös tuottaa helposti luettavaa ja ymmärrettävää tutkimusta, joka palvelee samalla myös kyberturvallisuuden popularisoinnin tarvetta ja laajempaa tietoisuuden kasvua. [8] [9] Tutkimus onkin aina tutkijansa näköinen.

[8] Tuomi et al. 2009, 55.
[9] Limnéll et al. 2014, 38-39.

## 2. AIHE JA TUTKIMUSKYSYMYS

Digitaalisessa maailmassa resurssit eivät enää yksinomaa määrittele valtioiden puolustuksen kyvykkyyttä ja kyberturvallisuuden ja kilpailun asymmetrisyys näkyykin kyberturvallisuuden tutkimuksessa keskeisenä ajatuksena. Digitaalisen hyökkäyksen ja puolustuksen kilpajuoksu[10] pohjaa entistä enemmän osaamiselle ja kyvylle innovoida uutta uuden disruptiivisen teknologian myötä. Esineiden internet, robotisaatio ja tekoäly tulevat uudelleen määrittelemään koko turvallisuuspoliittisen kentän tulevina vuosina. Muuttunut toimintaympäristö luo valtiollisille toimijoille paineen lisätä omaa turvallisuus- ja tiedustelutoimintaansa verkossa, mikä herättää usein keskustelua yksilöön liittyvästä tietosuojasta ja yksityisyyden suojasta.

Vaikka kyberturvallisuus on puhuttanut ja kirvoittanut paljon kirjallisuutta 2000-luvulta lähtien, on aiheen tutkimus yleistynyt vasta viimeisten vuosien aikana. Kyberturvallisuus on aihe, mikä läpileikkaa useita tieteenaloja informaatiotieteistä taloustieteeseen ja kansainväliseen politiikkaan sen uniikin luonteen vuoksi. Kyberympäristö on kaikkialla ja koskettaa jokaista usein eri tavoin; sosiaalisesti, poliittisesti, taloudellisesti sekä kulttuurillisesti. Kasvava riippuvuutemme tietoverkoista ja kybermaailmasta nostaa valtion uudenlaisen toimintaympäristön keskiöön. Koska kybermaailma ei tunnusta valtioiden rajoja, on sen toimintaympäristö perustaltaan kansainvälinen.

*Kyberturvallisuus ei rajaudu kansallisesti eikä kunnioita valtiorajoja. Toimijoiden joukossa on intresseiltään ja voimavaroiltaan erilaisia valtiollisia toimijoita sekä monenlaisia ei-valtiollisia toimijoita. Suomen kannanotot ja toiminta kyberturvallisuuteen liittyvissä kysymyksissä omalta osaltaan vaikuttavat Suomen kansainväliseen asemaan sekä Suomen kahdenvälisiin suhteisiin muiden valtioiden kanssa.* [11]

Kansainvälisen politiikan tutkijoille on siten tärkeää omaksua ja oppia ymmärtämään informaatioteknologian peruskäsitteitä osana oman tieteenalan tutkimusta.[12] Tieteellisessä tutkimuksessa uutta tietoa pyritään tuottamaan ymmärtämällä ilmiöitä eri teorioiden ja mallien

[10] mt. 2014, 22.

[11] Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2014, 2. ”Kansainvälisillä foorumeilla Suomen viiteryhmä poliittisissa kysymyksissä ovat muut demokratiaa, ihmisoikeuksia ja oikeusvaltioperiaatetta korostavat maat, erityisesti Euroopan unionin jäsenmaat sekä Pohjoismaat. Suomi toimii kyberturvallisuuteen liittyvissä kysymyksissä YK:n, Etyjin, Naton ja muiden kansainvälisten organisaatioiden ja prosessien puitteissa. Suomelle on tärkeää tukea EU:n yhteisten toimintalinjojen vahvistamista kyberturvallisuudessa, mukaan lukien EU:n kyberstrategiatyö”.

[12] Hansen & Nissenbaum 2009, 1172.

valossa.[13] Tässä tutkimuksessa pyritään siis ymmärtämään kyberturvallisuutta ilmiönä ja sitä miten ilmiö näyttäytyy *turvallistamisen kontekstissa.* Kyseessä on ennenkaikkea laadullinen tutkimus, jolla pyritään ymmärtämään kyberturvallisuutta reaalimaailman ilmiönä.

Tämän tutkielman tutkimuskohteena on Suomen kyberturvallisuusstrategia ja sen osana case esimerkkinä siviilitiedustelulainsäädännön eli tiedustelulain valmisteluun vuosina 2015-2018 liittyvä poliittinen keskustelu. Tarkoituksena on selittää ja selvittää sitä, millainen turvallistamisen prosessi Suomessa on kyberturvallisuuteen liittyen käynnissä ja millaisin diskurssein ja puheaktein turvallistamista tapahtuu.

Seuraava lainaus Suomen kyberturvallisuusstrategiasta vuodelta 2013 kiteyttää hyvin tämän tutkimuksen lähtökohdan:

*Kyberturvallisuus ei ole tarkoitettu oikeudelliseksi käsitteeksi, joka perustaisi uusia toimivaltuuksia viranomaisille tai muille toimielimille. Tältä osin ei ehdoteta muutoksia varautumisjärjestelyjen perusteisiin, eikä eri viranomaisten toimivaltamäärittelyihin.*[14]

Vain kaksi vuotta myöhemmin, olimme tilanteessa jossa nimenomaan kyberturvallisuuteen viitaten Suomen poliisi- ja puolustusviranomaisten tiedusteluvaltuuksia oltiin merkittävästi laajentamassa ja suojelupoliisille myöntämässä uusia toimivaltuuksia. Tätä tutkimusta ajaa kysymys siitä, mikä on se voima, joka saa aikaa näin suuren muutoksen, näin lyhyessä ajassa?

Koska tutkimuksen kohteena on turvallisuuspuhe ja ne diskurssit, joilla joko turvallisuuden tai uhkan mielikuvia vahvistetaan, on luontevaa valita tutkimusaineistoksi tekstidokumentteja. Laadullisen tutkimuksen ja diskurssianalyysin avulla pyritään vastaamaan kysymyksiin:

*”Millä tavalla kyberturvallisuudesta ja tiedustelulaista puhutaan julkisuudessa?”* ja
*”Millaisia päätelmiä tiedustelulaki -esimerkkiä käyttäen aineistosta tehtyjen havaintojen perusteella voidaan tehdä Suomen kyberturvallisuuskeskusteluun liitetystä turvallistamisprosessista?”*

Tavoitteena on analysoida ja tarkastella puheaktien valossa sitä, miten kyberturvallisuutta pyritään turvallistamaan poliittisessa diskurssissa ja pohtia sitä mikä merkitys turvallistamisyrityksellä on peilaten sitä laajempaan teoreettiseen viitekehykseen.

[13] Vilkka 2015, 19-22.
[14] Suomen kyberturvallisuusstrategia 2013, 2.

Tutkimuskohde on rajattu sekä aineistoon perustuen, että ajallisen ajanjakson perusteella. Tutkimuksen kohteena on Suomen kyberturvallisuusstrategia ja siviilitiedustelulainsäädännön valmistelu ja niihin liittyvä dokumentaatio. Keskeisen osan aineistoa muodostavat Suomen ensimmäinen kansallinen kyberturvallisuusstrategia[15] vuodelta 2013 ja tähän keskeisesti liittyvät strategiaa täydentävät toimenpideohjelmat vuosilta 2014-2016 ja 2017-2020. Tiedustelulakiin liittyvän tapaustutkimuksen lähdeaineistona on käytetty Sisäministeriön virallisia tiedotteita ja uutisia vuosilta 2015-2018, hanketietoja ja asiakirjoja kuten virallisia lausuntodokumentteja, sekä Perustuslakivaliokunnan mietintöä liittyen tiedustelulainsäädännön uudistukseen syksyllä 2018.

Toisen aineistokokonaisuuden muodostavat Helsingin Sanomien ja Ylen uutisten artikkelit vuoden 2015 lopulta vuoden 2018 syksyyn. Artikkelit käsittelevät tiedustelulainsäädännön uudistusta ja edustavat tapaustutkimukseen olennaisesti liittyvien toimijoiden kuten hallituksen ja sen jäsenten, tasavallan presidentin ja tiedustelulainsäädäntöön perehtyneiden oikeusoppineiden ja tutkijoiden näkökulmaa.

Tutkimuksen kohteena olevat dokumentit on kerätty ja löydettävissä pääasiallisesti viranomaislähteistä verkosta Valtioneuvoston ja Sisäministeriön verkkosivuilta ja toisaalta Yleisradion ja Helsingin Sanomien verkkosivuilta tiedustelulainsäädäntöä koskevasta uutisoinnista. Lähteinä on pyritty käyttämään mahdollisimman virallisia tietolähteitä kuten viranomaislähteitä mutta soveltuvin osin myös uutislähteitä, jotta voisimme muodostaa tutkimuksen kohteena olevasta ”turvallisuuspuheesta” mahdollisimman kattavan ja moniulotteisen käsityksen. Valtiollisten toimijoiden sivuilta, sekä eri uutislähteistä kootut dokumentit, tiedotteet ja uutiset on listattu tämän tutkielman aineistoluettelossa.

Samalla tutkimus läpileikkaa ja tuo esiin Suomen kyberturvallisuusstrategian lyhyen evoluution ja huomioi, että aiheeseen liittyvää tutkimusta on vielä verrattain vähän saatavilla sekä kansainvälisessä, että kotimaisessa kontekstissa. Yleisenä megatrendinä kyberturvallisuuden ja siihen liittyvien uhkien lisääntyminen on omiaan lisäämään tutkimusta aiheen ympäriltä tulevaisuudessa. [16]

[15] Suomen kyberturvallisuusstrategia 2013.
[16] Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017, 12.

Koska tämä tutkimus peilaa poliittista puhetta turvallistamisen teorian ja puheaktien kautta, on luontevaa ottaa diskurssianalyysi osaksi tutkimuksen tekemistä. Seuraavissa kappaleissa läpikäydään kielen merkitystä ymmärryksen ja todellisuuden tuottajana ja kriittisen diskurssianalyysin perustaa tämän tutkimuksen metodisena lähtökohtana.

### 2.2. Diskurssianalyysi merkityksen tulkitsijana

Kielellä on suuri merkitys siihen, miten jäsennämme ympärillämme vallitsevaa todellisuutta, joko konkreettista tai kuvitteellista. Käsitteiden, kuvausten, määritelmien, dialogin ja tarinoiden kautta maailmamme muodostuu erilaisista semioottisista merkityksistä, missä meillä jokaisella on merkittävä rooli ei vain merkitysten tulkitsijoina mutta myös merkitysten luojina.[17]

Kieli ja sen merkitykset eivät myöskään synny tyhjiössä. Siitä syystä, jos haluamme tutkia kieltä, joko puhuttua tai kirjoitettua, meidän on ymmärrettävä laajemmin, missä kontekstissa kieltä käytetään. Yhteiskunnalla, kulttuurilla, historialla, instituutioilla, politiikalla ja vallalla on kaikilla asemansa ei vain kielen tuottamisen kohteina vaan myös kieleen vaikuttavien merkitysten tuottajina.[18] Kielitiede yksinään ei riitä selittämään tai tutkimaan kieltä ja sen käyttöä yhteiskunnallisessa kontekstissa, mistä syystä kielitieteen ja yhteiskuntatieteiden välimaastoon on syntynyt oma tutkimusalueensa, jota kutsutaan diskurssianalyysiksi.

Diskurssianalyysi teoriana ja tutkimusmenetelmänä jakaantuu edelleen moniin eri haaroihin, joista osa keskittyy selittämään kielen kuvaamista ja merkityksiä ja osa kielen kielellä vaikuttamisen mahdollisuuksia poliittisessa, sosiaalisessa tai kulttuurillisessa kontekstissa. Diskurssianalyysin keskeisin merkitys syntyy siitä, että ymmärrämme tekevämme valintoja tuottaessamme puhetta tai tekstiä ja sitä kautta luovamme merkityksiä emme vain sillä mitä sanomme, mutta myös sillä mitä jätämme sanomatta.[19]

Tämä tutkimus tapahtuu kansainvälispoliittisessa viitekehyksessä ja sen avainasemassa ovat institutionaaliset, valtiolliset toimijat, joten on perusteltua ottaa tutkimuksen metodiseksi viitekehykseksi kriittinen diskurssianalyysi, joka huomioi kielenkäytön ja yhteiskunnan välisen toisiinsa vaikuttavan suhteen.

[17] James Paul Gee and Michael Handford teoksessa Routledge Handbook of Discourse Analysis 2012, 1-3.
[18] mt. 2012, 5.
[19] James Paul Gee and Michael Handford teoksessa Routledge Handbook of Discourse Analysis 2012, 5.

Kriittiselle diskurssianalyysille on ominaista pyrkiä löytämään merkityksiä, jotka kätkeytyvät diskurssin sisään. Kriittisen diskurssianalyysin tunnetuimpiin teoreetikkoihin lukeutuva Norman Fairclough esittää kriittisen diskurssianalyysin tutkimuskohteeksi semiotiikan ja muiden sosiaalisten elementtien relaatiot, jotka vaihtelevat riippuen kulloinkin vallitsevista olosuhteista ja käsiteltävistä instituutioista tai organisaatioista. Kriittinen diskurssianalyysi tutkimuksena on siten aina ajasta ja paikasta riippuvaista.[20] Diskurssintutkimuksen kantavana ajatuksena on se, että todellisuutta tai eri asioita merkityksellistetään tarkoitushakuisesti ja analyysin keinoin diskurssien tutkijat pyrkivät selvittämään, miten tämä tapahtuu ja mitä seurauksia asioiden merkityksellistämisellä mahdollisesti on. [21]

Diskurssien ja tekstien tutkimuksessa on hyvä ymmärtää myös tutkimusotetta ja eri koulukuntien tapoja mieltää vallitsevaa todellisuutta. Realisteille maailma näyttäytyy niin kuin se on ja realistinen tulkinta antaa ymmärtää, että on olemassa yksi, vallitseva totuus ja muiden (eriävät) tulkinnat ovat vääriä. Strukturalistit taas ymmärtävät, että esimerkiksi eri kulttuureissa asioita tulkitaan eri tavoin mutta strukturalistit olettavat, että eroavaisuuksien alla ihmisillä on joukko yleistettävissä olevia perusominaisuuksia, jotka ovat inhimillisesti kaikilla samat. Post-strukturalismi sen sijaan ei pyrikään selittämään ja yleistämään tulkintoja vaan lähestymistapa ymmärtää kontekstuaaliset ja kulttuuriset erot tulkinnoissa ja hyväksyy sen, että yhden totuus ei välttämättä ole toisen totuus ja että ihmiset tulkitsevat todellisuutta tosiasiallisesti hyvin eri tavoin. [22]

Kriittinen diskurssianalyysi on luonteeltaan post-strukturalistista, sen tarkoituksena ei ole selvittää kenen versio totuudesta on oikein vaan se keskittyy selvittämään erilaisten totuuksien painoarvoa, millaiset merkitykset kullakin hetkellä ovat vallalla, samalla kun toiset merkitykset sivuutetaan mahdollisesti kokonaan.[23] Kieltä ja diskursseja tutkimalla voidaankin oppia paljon ympäröivästä yhteiskunnasta ja tietyn ajanhetken ilmiöistä.[24]

Samalla tapaa tämä tutkimus pyrkii diskursseja tutkimalla oppimaan ja tulkitsemaan miten kyberturvallisuutta merkityksellistetään ja turvallistetaan yhteiskunnallisena ilmiönä. Tässä yhteydessä erityisesti kielenkäyttäjän kielelliset ja diskursiiviset valinnat nousevat erityisen

[20] Norman Fairclough teoksessa Routledge Handbook of Discourse Analysis 2012, 10-11.
[21] Sari Pietikäinen et al. 2009, 10.
[22] McKee 2003, 9.
[23] Pietikäinen et al. 2009, 10.
[24] mt. 2009, 11.

merkityksellisiksi. Sanavalinnoilla ja kielellisillä resursseilla rakennetaan merkityksiä kontekstin sallimissa rajoissa, millä tarkoitetaan sitä, että erilaiset yhteiskunnalliset normit, arvot ja toisaalta institutionaaliset arvot ja normit vaikuttavat aina taustalla kun kieltä tuotetaan tietyssä tilanteessa.[25]

Kriittisen diskurssintutkimuksen ytimessä on kaksi toisistaan eroavaa diskurssin käsitettä. Yleisenä ja yksikkömuotoisena diskurssilla viitataan kaikkeen kielelliseen vuorovaikutukseen, johon liittyy jonkinlaisia sosiaalisia ehtoja tai odotus seurauksesta. Tässä diskurssin merkityksessä kieli nähdään toimintaan tilannesidonnaisena resurssina. Jos taas diskursseista puhutaan monikossa, viitataan vakiintuneisiin eri kieliyhteisöissä syntyneisiin merkityksellistämisen tapoihin, jotka ovat tunnistettavia ja suhteellisen muuttumattomia.[26] Näin diskursseja esiintyy samanaikaisesti kahdessa ulottuvuudessa, mikrotasolla kielellisenä ilmiönä ja makrotasolla kontekstisidonnaisena toimintana.

Diskursseja tutkimalla voidaan havainnoida erilaisia makrotasolla vaikuttavia prosesseja ja sääntöjä. Tämän tutkimuksen kannalta tärkeämpää on kuitenkin huomioida se, että diskursseja on mahdollista tutkia myös toisin päin, tarkastelemalla sitä miten makrotason prosesseja eli tässä tapauksessa kyberturvallisuutta merkityksellistetään eri teksteissä ja eri konteksteissa. [27] Asiat ja ilmaisut saavat merkityksen vasta kun ne pystytään liittämään tiettyyn kontekstiin. Yksittäiset ilmaisut voivat saada eri painoarvon ja merkityksen kun niitä analysoidaan suhteessa eri konteksteihin. Kontekstilla taas viitataan laajemmin esimerkiksi yhteiskunnalliseen tilaan, toimintaympäristöön tai asiayhteyteen. Merkitykset syntyvät tiettyjen elementtien vaikutuksessa, jotka mahdollistavat mutta myös rajaavat tulkintojen muodostumista.[28]

Juuri diskurssien kontekstisidonnaisuuden vuoksi on tutkimuksellisesta näkökulmasta tärkeää pystyä rajaamaan se konteksti, jossa diskursseja tutkitaan. Samanaikaisesti on ymmärrettävä, että kontekstitkin ovat monikerroksisia ja vaikka rajaisimme tutkimuksen johonkin tiettyyn tilannekontekstiin, on syytä tunnistaa myös muut läsnä olevat kontekstit, jotka voivat olla esimerkiksi institutionaalisia, historiallisia tai yhteiskunnallisia.[29]

[25] mt. 2009, 13.
[26] mt. 2009, 20.
[27] Pietikäinen et al. 2009, 22.
[28] mt. 2009, 24.
[29] mt. 2009, 24.

Diskurssianalyysi pyrkii yhdistämään eri käsitteitä, sekä ilmiön mikro- että makrotasot teoreettiseen perspektiiviin, mikä tässä tutkimuksessa tarkoittaa muun muassa turvallisuus -käsitteen kytkemistä kyberturvallisuus ilmiöön sekä turvallistamisen teoriaan. Olennainen osa tutkimusprosessia on sillan rakentaminen näiden elementtien välille ja sen ydinkohdan, neksuksen, tunnistaminen missä eri tasot ja näkökulmat yhdistyvät siten, että kaikilla elementeillä on oma vaikutuksensa merkityksen syntymiseen.[30]

### 2.1.1. Diskurssit ja representaatio

Diskursseilla rakennetaan käsitystä ympäröivästä todellisuudesta ja maailmasta ja juuri tässä kyvyssä piilee diskurssien ja diskurssianalyysin merkityksellisyys. Kyky kuvata eli representoida maailmaa diskurssien avulla on voimakas vallankäytön väline, etenkin jos huomioimme diskurssille sen ominaisen luonteen, eli diskurssien rakentumisen valintojen kautta. Yhtä merkityksellistä kuin se, mitä asioita diskurssiin sisällytetään, on se, mitkä asiat on tietoisesti jätetty diskurssista pois.[31]

On myös mahdollista, että samaa ilmiötä tulkitaan useasta eri lähtökohdasta eli samanaikaisesti esiintyy useita eri diskursseja, joista toiset voivat olla enemmän vallalla. Nämä diskurssit edustavat tyypillisesti eri näkökulmia samasta aiheesta. Diskursseja käyttämällä organisoidaan merkityksiä ja rakennetaan kuvaa, representaatiota, diskurssin kohteena olevasta aiheesta sekä samanaikaisesti myös siihen liittyvistä toimijoista, näiden identiteeteistä ja toimijoiden välisestä dynamiikasta.[32] Tietty diskurssi tuo näkyviin vain tietyn näkökulman.[33]

Representaatiolla viitataan siis siihen, miten kielen avulla kuvataan maailmaa. Representaatio juontuu sanasta uudelleenesittää, millä puolestaan viitataan siihen kuinka silloin kun asioita esitetään uudelleen, nojaamme olemassaolevaan tietoon ja aikaisempiin esityksiin samasta aiheesta. Toisaalta jokainen representaatio on oma, ainutlaatuinen ja ajallinen tulkintansa. Representaation avulla voidaan tutkia sitä, miten jokin ilmiö rakentuu, eri näkökulmista ja eri keinoin.[34]

[30] mt. 2009, 108.
[31] mt. 2009, 41-42.
[32] Pietikäinen et al. 2009, 42.
[33] mt. 2009, 43.
[34] mt. 2009, 43.

Myös representointiin pätee määritelmä toiminnasta, jolla on ehtoja ja seurauksia. Se herättää myös kysymyksiä vallasta, esimerkiksi siitä mitä osia diskurssista tehdään näkyväksi ja mitä ei, ja toisaalta, kenellä on oikeus ja valta tehdä näitä valintoja?[35] Myös representaatiot ovat kontekstisidonnaisia ja heijastelevat aina aiempia representaatioita.[36] Tiettyä aihetta tai ilmiötä tutkittaessa läsnä on useasti useampi diskurssi. Tämä tulkinta vahvistuu myös tämän tutkimuksen edetessä. Nämä diskurssit ovat harvoin kuitenkaan samanarvoisessa asemassa vaan ne asettuvat hierarkkiselle arvoasteikolle sen perusteella mikä diskurssi milläkin ajanhetkellä on vallassa. Tämä diskurssien valtajärjestelmä on jatkuvasti liikkeessä ja niiden merkitykset muuttuvat tilanteen ja kontekstin mukaan.[37]

Diskursiivista valtaa tutkittaessa on huomioitava myös käsitteenä diskurssijärjestys. Diskurssijärjestyksellä tarkoitetaan sitä miten diskurssit järjestäytyvät semioottisten rakenteidensa ulkopuolella eli sosiaalisin tai yhteiskunnallisin perustein. Tämä on merkityksellistä siitä syystä, että järjestäytyminen määrittelee sen, mitkä diskurssit pääsevät ääneen ja mitkä pyritään vaientamaan.[38] Eri toimijoiden diskurssit eivät ole keskenään samanarvoisia, osin kieleen ja sen kautta rakentuvan luottamusjärjestelmän vuoksi. Olemme tottuneet pitämään joidenkin toimijoiden diskursseja luotettavampina kuin toisten, käsitys mikä on rakentunut aikaisempien representaatioiden ja kokemusten kautta.[39]

Lähdemme liikkeelle siitä, miten turvallisuuden kokemuksemme syntyy, miten kyberturvallisuus on käsitteellistetty ja miten turvallistamisen teoria näkee erilaiset asiat turvallisuuttamme uhkaavina asioina aina intersubjektiivisen kokemuksen ja tiettyyn ajanhetkeen sidonnaisina, omalta osaltaan diskursiivisina ja yhä uudelleen konstruoituvina elementteinä. Jo tässä vaiheessa voimme todeta, että jos haluamme ymmärtää kyberturvallisuutta ilmiönä ja pyrkiä selittämään sitä turvallistamisen teorian kautta, pitää meidän tulkita puhetta ja keskustelua, jota ilmiön ympärillä käydään.

Puhe tai paremminkin *puheaktit* politiikan teon välineenä rakentuvat erilaisten diskurssien päälle. Turvallistamisen teoria tunnistaa eri turvallisuuden sektoreilla erilaisia tapoja konstruoida todellisuutta tiettyjen kielellisten lainalaisuuksien tai konseptien avulla.

[35] mt. 2009, 43.
[36] mt. 2009, 44.
[37] mt. 2009, 44.
[38] mt. 2009, 46.
[39] Pietikäinen et al. 2009, 46.

Kyberturvallisuutta ja turvallistamisen teoriaa tutkineet Lene Hansen ja Helen Nissenbaum ovat esittäneet kyberturvallisuussektorille omia diskursiivisia konseptejaan, jotka esitellään tarkemmin luvussa 3.7.

# 3. ANALOGISESTA TURVALLISUUDESTA KOHTI DIGITAALISTA TURVALLISUUTTA

Ennen kuin sukellamme syvemmin turvallisuudentutkimuksen perinteeseen, on tarpeen selittää ja selvittää sitä miten turvallisuuden kokemuksemme ylipäätään syntyy ja miten kyberturvallisuus haastaa perinteisen turvallisuuden mallin.

Turvallisuus käsitetään perinteisesti syy-seuraussuhteiden kautta. Turvallisuutta uhkaa jokin syy, jolla toteutuessaan on seuraus, mitä pyrimme välttämään. Kyberturvallisuus on kuitenkin alue, joka hämärtää rajat olemassaolevan ja todellisen, sekä aineettoman, kuvitteellisen välillä.[40] Kybermaailma on samaan aikaan turvallisuutta potentiaalisesti uhkaava ja kuitenkin nykymaailmankuvassa olennainen osa turvallisuuttamme. Kyberturvallisuus on siis uuden *tilan* turvattomuutta, sekä käytäntöjä ja prosesseja, joilla siitä yritetään tehdä turvallisempaa. Sillä viitataan sekä tekniseen, että ei-tekniseen tekemiseen, jotka on tarkoitettu sähköisen ympäristömme ja siihen liittyvän datan suojelemiseen kaikilta mahdollisilta uhkatekijöiltä.[41]

Tämän tutkimuksen ylätason teoreettisena viitekehyksenä käytetään turvallistamisen teoriaa. Jotta voimme ymmärtää turvallistamisen teoriaa, pitää ensin avata turvallisuuden ja turvallistamisen ontologiaa ja epistemologiaa, sitä mitä turvallisuus oikeastaan on ja miten käsityksemme turvallisuudesta syntyy. Tutkimuksen keskeisiä käsitteitä ovatkin turvallisuus ja kyberturvallisuus, joita avataan tarkemmin seuraavassa luvussa.

## 3.1. Kyberturvallisuus perinteisen turvallisuudentutkimuksen haastajana

Turvallisuus käsitteenä on helpoimmin ymmärrettävissä vastakohtansa, uhkan kautta. Turvallisuus on se tila, jossa emme koe uhkaa. Uhka on siten ymmärrettävissä tekijänä, joka aiheuttaa vaaraa, haittaa tai epävarmuutta toimintaympäristössämme.[42] Kyberturvallisuutta tutkineet Jarno Limnéll, Klaus Majewski ja Mirva Saarinen ovat kuvanneet turvallisuutta tunteen, todellisuuden, opittujen mallien ja sietokyvyn yhdistelmänä. Turvallisuus onkin aina subjektiivinen kokemus, johon yhdistyy faktapohjaista tilannekuvaa, arvoja ja toimintamalleja

[40] Lobato et al. 2015, 25-26.
[41] Cavelty 2012b, 5 artikkelissa Lobato & Kenkel 2015, 25-26.
[42] Limnéll et al. 2014, 34.

sekä kykymme sietää erilaisia häiriötekijöitä.[43] Tapamme käsitellä turvallisuutta sitä uhkaavien tekijöiden kautta, asettaa uhkien arvioinnin ja suhteuttamisen meille tärkeisiin arvoihin nähden koko turvallisuudenkokemuksen rakentamisen lähtökohdaksi[44].

Turvallisuuteen, samoin kuin kyberturvallisuuteen, liitetään kolme ulottuvuutta, jotka ovat turvallisuuden tuottamisen keskiössä. *Kohde* määrittelee sen, mitä turvataan, *uhka* määrittelee sen miltä turvataan ja *keinot* sen, miten kohdetta pyritään turvaamaan.[45]

Kyber[46] on käsite, joka harvoin ilmenee yksinään ja esiintyy useammin yhdyssanan etuliitteenä esimerkiksi sanojen -todellisuus, -turvallisuus ja -uhka yhteydessä. Kyberillä viitataan kuitenkin yleisesti todellisesta maailmasta erotettavissa olevaan keinotekoiseen bittiavaruuteen ja digitaaliseen toimintaympäristöön.[47] On kuitenkin huomioitava, ettei kyberiä voida kokonaan irrottaa fyysisestä todellisuudesta, siksi kyber viittaakin myös fyysisen ja digitaalisen rajapintaan ja näiden kahden todellisuuden yhä voimistuvaan keskinäisriippuvuuteen. [48]

Länsimaisen sivistysvaltion tullessa yhä riippuvaisemmaksi kybertodellisuudesta ja digitalisaation mahdollistamista ratkaisuista, kasvaa myös odotuksemme tämän uuden hybriditodellisuuden turvallisuudesta. Kansalaisina meidän pitää pystyä luottamaan siihen, että valtio yhteiskunnan ylimpänä turvallisuustoimijana huolehtii myös tämän uuden todellisuuden elinkelpoisuudesta ja toimintaedellytyksistä samoin kuin fyysisestä todellisuudestamme.[49] Tätä uutta turvallisuuden ulottuvuutta kutsutaan kyberturvallisuudeksi.[50]

### 3.2. Kyberturvallisuuden tutkimus

Kylmän sodan päättymisen jälkeen geopoliittisten jännitteiden lauettua ja teknologian nopean kehityksen siivittämänä turvallisuuspoliittinen agenda muutti nopeasti muotoaan.[51] Turvallisuuden tutkimus osana kansainvälisen politiikan tutkimusaluetta nousi nopeasti

[43] mt. 2014, 34-35.
[44] mt. 2014, 37.
[45] mt. 2014, 37-38.
[46] Sana kyber juontuu kreikan sanasta kybereo, mikä tarkoittaa opastamista, ohjaamista ja hallintaa.
[47] Limnéll et al. 2014, 29.
[48] mt. 2014, 31.
[49] mt. 2014, 31-32.
[50] Jarno Limnéllin, Klaus Majewskin ja Mirva Salminen ovat muotoilleet kirjassaan Kyberturvallisuus (2014) käsitteen seuraavasti: Kyberturvallisuus tarkoittaa digitaalisen maailman tilaa, jossa vallitsee sekä ymmärryksen myötä tuotettu luottamuksen tunne että käytännön toimenpitein saavutettu kyky ennakoivasti hallita sekä sietää kyberuhkia ja niiden vaikutuksia (alkup. kursivointi poistettu).
[51] Hansen & Nissenbaum 2009, 1155.

yhdeksi tutkituimmaksi alueeksi jokaisen kolmen suuren kansainvälisen politiikan koulukunnan - realismin, liberalismin ja konstruktivismin näkökulmasta pyrkiessä ymmärtämään muuttunutta maailmanjärjestystä. [52] Teoreetikoista muun muassa Johan Eriksson ja Giampiero Giacomello ovat omissa politiikan ja turvallisuuden tutkimuksissaan tarkastelleet sitä, miten tietoyhteiskunnan nousu ja kyberturvallisuuden käsitteen syntyminen ovat vaikuttaneet kansainvälisen politiikan turvallisuuden tutkimukseen.[53]

Erikssonin ja Giacomellon mukaan suurin osa tutkimuksesta, joissa on liitetty kansainvälinen politiikka, turvallisuuden tutkimus ja informaatioteknologia toisiinsa, on aihetta lähestytty empiirisesti ja erilaisten teoreettisten käsitteiden kautta onnistumatta kuitenkaan linkittämään tutkimusta mihinkään olemassa olevaan kansainvälisen politiikan teoriaan.[54] Eriksson ja Giacomello väittävätkin, että samaan aikaan kun 2000-luvun turvallisuudentutkimus on keskittynyt käymään debattia itse turvallisuuden käsitteestä traditionaalisen turvallisuudentutkimuksen ja laajan turvallisuuskäsitteen kannattajien välillä, jättivät eri teoriat tietoyhteiskunnan nousun ja digitalisaation pitkään huomioimatta.[55]

Realisteille, turvallisuudentutkimus ja kyberturvallisuus sen osana nojaavat edelleen vahvasti kansallisvaltion käsitteeseen ja turvallisuuden ymmärtämiseen ensisijaisesti sotilaallisen voimankäytön kautta.[56] Realistit ovatkin kyberturvallisuuden tutkimuksessaan lähinnä kiinnostuneita informaatiosodankäynnistä, minkä voidaan katsoa pääsääntöisesti tapahtuvan kahden eri valtion välillä, pyrkimyksenä vaikuttamaan toisen valtion asioihin ja siten strategisena ja sotilaallisena toimintana. Realisteille kyberturvallisuus edustaakin ennemmin teorian jatkuvuutta, kuin sen dramaattista muutosta, missä kyberturvallisuuskin voidaan määritellä vastustajien sekä hyökkäyksen ja puolustuksen kautta vaikkakin uudenlaisessa ulottuvuudessa.[57]

Liberalistit, sen lisäksi, että tunnustavat valtion keskeisen roolin maailmanpolitiikassa, huomioivat myös monien muiden toimijoiden aseman kansainvälisissä suhteissa. Erilaiset valtioiden rajat ylittävät suuryritykset ja monikansalliset toimijat, yhteiskunnalliset liikkeet ja valtioista riippumattomat toimijat, yhteistyöverkostot tai terroristijärjestöt ovat kaikki

[52] Eriksson et al. 2007, 3.
[53] mt. 2007, 3.
[54] mt. 2007, 4.
[55] Eriksson et al. 2007, 9-10.
[56] mt. 2007, 12.
[57] mt. 2007, 12.

kansainvälisen politiikan toimijoita, jotka vähentävät kansallisvaltion ja sen suvereniteetin merkitystä maailmanpolitiikassa.[58] Liberalistit korostavat kollektiivista ja yhteistyöhön perustuvaa turvallisuutta, erityisesti erilaisten ylikansallisten toimijoiden kuten YK:n koordinoimana.[59]

Liberalistien painottama keskinäisen riippuvuuden käsite päivitettiin 2000-luvulla kattamaan myös keskinäisriippuvuudesta syntyvät ”kustannukset” eli herkkyyden ja haavoittuvuuden, joskin nämä uudet käsitteet esitettiin vain taloudellisesta perspektiivistä, eikä kansalliseen tai kansainväliseen turvallisuuteen vaikuttavina tekijöinä.[60] Eriksson ja Giacomello näkevät kaksi liberaaliin teoriaan sopivaa modernia sosioekonomista trendiä merkityksellisinä myös digitaalisen turvallisuuden tutkimuksen näkökulmasta; ensinnäkin yksityisen- ja julkisen sektorin lähentymisen ja kumppanuussuhteiden perustamisen palvelujen tarjoamiseksi sekä siviili- ja sotilaallisen vaikutuspiirin yhteensulautumisen. Määräysvallan ja vastuun rajat ovat monissa tapauksissa hämärtyneet, eivätkä valtiot enää yksinään pysty vastaamaan kansallisen turvallisuuden tarpeeseen ilman yksityisen sektorin tukea.[61] Erikssonin ja Giacomellon mukaan liberalistisen koulukunnan edustajista vain Arquilla ja Ronfeldt (2001) ovat ainoita, jotka ovat globalisaation ja muiden valtion suvereniteettia haastavien asioiden lisäksi käsitelleet erityisesti toimijoiden pluralistisuutta kyberturvallisuuden näkökulmasta.[62]

Konstruktivismi nousi kansainvälisen politiikan tutkimukseen 1980-luvun loppupuolella. Konstruktivisteille kylmän sodan jälkeinen uusi maailmanjärjestys tarjosi hedelmällisen maaperän kun kansainvälisen politiikan tutkimuksen valtateoriat ajautuivat kriisiin, epäonnistuessaan selittämään meneillään olevaa politiikan paradigman muutosta.[63] Konstruktivistit korostavat todellisuuden tulkinnanvaraisuutta ja argumentoivat, että materiaalisen maailman lisäksi sosiaalinen todellisuutemme on sosiaalisesti konstruoitua, normeihin, arvoihin ja identiteetteihin perustuvaa rakennettua todellisuutta, joka riippuu ja vaihtelee kulloinkin vallitsevista olosuhteista.[64]

[58] mt. 2007, 13.
[59] mt. 2007, 14.
[60] Ks. Eriksson et al. 2007, 14-15. Joseph Nye ja Robert Keohane esittelivät 1970-luvulla kompleksisen keskinäisriippuvuuden (eng. complex interdependency).
[61] Eriksson et al. 2007, 15-16.
[62] mt. 2007, 17.
[63] mt. 2007, 17.
[64] mt. 2007, 18.

Konstruktivismi ei varsinaisesti ota kantaa siihen, mikä ja milloin ja miten jokin asia voidaan katsoa turvallisuusongelmaksi tai miten tällaiseen uhkaan tulisi vastata, vaan keskittyy tutkimaan sitä, *miten* jokin asia muodostuu turvallisuusongelmaksi. Kuten Eriksson ja Giacomello asian esittävät, konstruktivisteilla paino onkin toimintaa ilmaisevassa ”muodostaa[65]” verbissä.[66] Konstruktivistit ovat kuitenkin se ryhmä, jotka ovat kehittäneet turvallisuuden tutkimukseen oman lähestymistavan, mitä kutsutaan *turvallistamisen* teoriaksi.[67] Tätä omaa teoreettista koulukuntaa kutsutaan Kööpenhaminalaiseksi koulukunnaksi.[68]

## 3.3. Kööpenhaminalainen koulukunta

Kööpenhaminalainen koulukunta nojaa kolmeen teoreettisen lähtökohtaan. Sen pohjana on turvallisuusteoreettinen debatti siitä, pitäisikö turvallisuus käsittää laajemmin kuin valtiollisen ja sotilaallisen toimijuuden kautta, yhtenä keskeisenä vaikuttimena puheaktin teoria ja yhtäältä Smithiläinen käsitys valtiosta ja turvallisuuspolitiikasta.[69] [70]

Näistä lähtökohdista syntyy ”turvallisuuden” käsite, joka nousee kansallisesta turvallisuusdiskurssista ja nojaa ajatukseen auktoriteetista ja tätä uhkaavasta vihollisesta, kyvykkyydestä toimia ja tehdä päätöksiä hätätoimenpiteiden toimeenpanosta[71] Turvallisuusdiskurssin ja turvallistamisen tutkimuksessa olennaista ei ole pyrkiä tekemään analyysia siitä, onko jokin asia turvallisuusuhka vai ei, vaan sen tarkoituksena on ymmärtää ne prosessit, jotka konstruoivat yhteistä ymmärrystä siitä mitä pidetään uhkana, ja siitä millainen rooli eri toimijoilla on tämän prosessin aikana.[72]

### 3.3.1. Turvallistamisen politiikkaa

Turvallistamisen teoria pohjaa konstruktivismiin, post-strukturalismiin ja kriittiseen teoriaan pyrkimyksenään selittää niitä rakenteita ja prosesseja, jotka vaikuttavat uhkien syntymiseen.

[65] Eng. verbi *become,* muodostua, tulla joksikin
[66] Eriksson et al. 2007, 19.
[67] mt. 2007, 19.
[68] mt. 2007, 19.
[69] Hansen & Nissenbaum 2009, 4.
[70] Huysmans 2006, 124-144.
[71] Hansen & Nissenbaum 2009, 4.
[72] Buzan et al. 1998:26, 34 kirjassa Eriksson & Giacomello 2007, 60.

Teorian mukaan mikään uhka ei siis ole uhka syntyessään vaan ajatus on, että jokin kohde turvallistetaan vasta poliittisen diskurssin kautta. Turvallistamisen teoria jakaantuu itsessään eri koulukuntiin, Kööpenhaminalaiseen konstruktivistiseen koulukuntaan, joka edustaa filosofista ja post-strukturalistista näkemystä kielestä ja sen merkityksestä diskurssien synnyssä ja toisaalta sosiologiseen koulukuntaan, jonka mukaan turvallistamista tulee tarkastella pragmaattisemmin, voimakkaasti kontekstisidonnaisena puhujan ja kuulijan välisenä vuorovaikutuksena.[73]

Turvallistamisen teorian keskeisiä teoksia on Barry Buzanin kirja Security: A New Framework for Analysis, missä turvallistamista käsitellään *puheakteina* ja poliittisen pelinteon välineenä.[74] Tämän mukaan retorisin keinoin jokin asia tai kohde, joka ei entuudestaan ole ollut valtion turvallisuutta uhkaava, *turvallistetaan* retorisin keinoin poliittisessa keskustelussa välittömiä toimia tai vahvaa johtajuutta vaativaksi ongelmaksi[75] pyrkimyksenä lopettaa aiheesta käytävä poliittinen keskustelu ja hyväksyä valtioiden toimenpiteet ilman yhteiskunnallista ja kriittistä keskustelua.

Buzan, Wæver ja Wilde kuvaavat turvallistamista eksistentialistisen uhan kautta, jotta jokin asia nousee turvallisuusuhkaksi, tulee sen uhata laajemmin olemassaoloamme tai toimintavapauttamme.[76] Teoria argumentoi vahvasti laajennetun turvallisuuskäsityksen puolesta, sen että olemassaoloomme tai turvallisuuteemme vaikuttavat tekijät voivat olla yhtä lailla ympäristöuhkia, taloudellisia- tai uskonnollisia uhkia sotilaallisen uhkan lisäksi.[77]

Tärkeää on huomioida se, että uhkan ei tarvitse välttämättä olla todellinen, riittää että uhka esitetään turvallistettuna, olemassaoloamme tai vallitsevaa nykytilaamme uhkaavana.[78] Myös Thierry Balzacq lähestyy turvallistamista pragmaattisena prosessina; jotta jokin konsepti voidaan turvallistaa, edellyttää se laajaa hyväksyntää sille, että tietty asia kehittyy uhkaavaan suuntaan siten, että yleisö sen hetkisen ymmärryksensä valossa, hyväksyy että kyseessä on asia tai ongelma, joka vaatii välittömiä toimia ongelman rajaamiseksi.[79]

[73] Balzacq 2011, 1-2.
[74] Korhonen teoksessa Politiikan Nykyteoreetikkoja 2008, 249.
[75] mt. 2008, 249.
[76] Vrt. esim. ilmastonmuutos.
[77] Hansen & Nissenbaum 2009, 1156.
[78] Buzan et al. 1998, 24.
[79] Vultee teoksessa Balzacq 2011, 77-78.

Turvallistamisen prosessia ja sen eri asteita kuvataan usein janana. Buzan, Wæver ja de Wilde esittävät teoriassaan, että periaatteessa mikä tahansa julkinen asia voidaan sijoittaa janalle sen mukaan, kuinka politisoituna asia esiintyy julkisessa keskustelussa. Janan toiseen ääripäähän sijoittuvat asiat, jotka eivät ole politisoituja, eivätkä siten julkisen keskustelun tai väittelyn piirissä, keskellä ovat politisoidut asiat, jotka vaativat valtion tai valtiollisen toimijan toimenpiteitä ja päätöksentekoa ja janan toisessa ääripäässä turvallistetut asiat, asiat jotka vaativat hätätoimenpiteitä ja joilla voidaan perustella tavanomaisesta poliittisesta prosessista poikkeamista.[80]

Kotimaisessa kontekstissa teoriaa tutkinut Pekka Korhonen esittää, että demokraattisissa valtioissa, esimerkiksi Suomessa, turvallisuuspolitiikasta voidaan keskustella julkisuudessa, mutta käytännössä keskustelu on rajoittunutta ja karttaa arkoja aiheita.[81] Suomessa viimeaikaisempia esimerkkejä turvallisuuspolitiikasta ja puheenteon dynamiikasta voi löytää Suomen Venäjä – suhteesta. Tässä tutkimuksessa lähtökohtana on, että sama turvallistamisen politiikka ja puheenteon dynamiikka ulottuu myös kyberturvallisuudesta käytävään keskusteluun, mistä pyritään löytämään mahdollisia viitteitä tutkimusaineistoa läpikäydessä.

Toinen tärkeä huomio, jonka Pekka Korhonen esittää turvallistamisesta, liittyy uhkaan ja sen argumentointiin. Niin kauan kuin turvallistamisen argumenttia ei ole hyväksytty, ei kyseessä ole onnistunut turvallistamisoperaatio vaan voidaan puhua turvallistamisyrityksestä.[82] Onkin mielenkiintoista nähdä, tuleeko tutkimukseni tuloksissa esiin selviä viitteitä siitä, missä vaiheessa turvallistamisen janalla Suomessa kyberturvallisuuskeskustelua käydään.

Turvallistamista on kohtalaisen suoraviivaista tutkia; retoriikasta ja diskurssista on mahdollista löytää semioottisia rakenteita, joilla on riittävä vaikutusvalta ihmisiin ja joiden perusteella yleisö hyväksyy sääntöjen taivuttamisen tai oikeuksien loukkaamisen, normaalista poiketen, määritellyn uhkan välttämiseksi.[83] Buzan, Wæver ja de Wilde muistuttavat meitä kuitenkin siitä, että vaikka turvallistamisen logiikka on selkeä, tulee meidän olla tietoisia siitä, milloin jokin asia katsotaan turvallistetuksi ja milloin puhutaan turvallistamisyrityksestä.[84] [85]

[80] Buzan et al. 1998, 23-24.
[81] Korhonen teoksessa Politiikan Nykyteoreetikkoja 2008, 250.
[82] Korhonen teoksessa Politiikan Nykyteoreetikkoja 2008, 251.
[83] Buzan et al. 1998, 25.
[84] Buzan et al. 1998, 25.
[85] Korhonen teoksessa Politiikan Nykyteoreetikkoja 2008, 251.

Näiden kahden erona voidaan pitää sitä, miten laaja yleisö niihin suhtautuu. Kun yleisön katsotaan hyväksyvän jonkin asian tai esimerkiksi mahdollisuuden hätätoimenpiteisiin turvallistamisen seurauksena, voidaan puhua turvallistetusta turvallisuusuhkasta. Yleisön käsite ja merkitys turvallistamisen teorialle on myös yksi eniten kritiikkiä herättäneitä asioita mutta tämän tutkimuksen näkökulmasta katsottuna riittää, että määrittelemme yleisön Wæverilaisittain siten, että yleisöllä täytyy olla riittävät edellytykset legitimoida turvallistamisyritys eli antaa hyväksyntänsä esitetyille toimenpiteille.[86] [87] [88]

Edelleen, korostaisin kuitenkin sitä, että turvallistamista saattaa tapahtua, vaikkei synnytetty uhkakuva todellisuudessa muodostaisi uhkaa tai vaatisi käytännössä koskaan hätätoimenpiteitä, riittää että uskomme siihen, että tällainen uhkan mahdollisuus on olemassa ja hyväksymme poikkeustoimet uhkakuvan toteutumisen estämiseksi.[89]

Turvallisuudessa ja turvallistamisessa korostuu siis kiireellisyyden tuntu. Kööpenhaminalainen koulukunta korostaakin, että turvallisuusdiskurssi voi synnyttää muitakin turvallistamisobjekteja valtion tai kansakunnan lisäksi ja kytkeä muitakin kuin sotilaallisen turvallisuuden sektorin keskusteluun niin kauan kuin tämä tapahtuu kansallisen/kansainvälisen draaman sävyttämänä ja laajemman yleisön hyväksymänä.[90]

### 3.3.2. Kenellä on lupa tuottaa turvallisuuspuhetta?

Kun käsitellään turvallistamista, on merkityksellistä huomioida, että asia tai uhka ei synny tyhjiössä itsekseen vaan vaatii aina aktorin tai toimijan puheaktin. Sana *turvallisuus* ei määrittele jonkin asian turvallisuutta tai uhkaavuutta. Turvallistamisessa korostuvat toiminta, joko välittöminä tai laajemman yleisön hyväksyminä toimenpiteinä, joilla vastataan uhkaan.[91] Tärkeää onkin esittää kysymyksiä siitä, kuka voi tehdä tai puhua turvallisuustekoja, mistä aihealueista ja millä määritelmillä?[92]

[86] Vuori 2008, 72.
[87] Mcdonald 2008, 564.
[88] Balzacq 2009, 7.
[89] Buzan et al. 1998, 25.
[90] Hansen & Nissenbaum 2009, 5.
[91] Buzan et al. 1998, 27.
[92] mt. 1998, 27.

Turvallistamisen prosessi vaatii aina *aktorin*, jonkun tahon, joka käyttää valtaansa tietyn asian turvallistamiseen. Tyypillisesti tällaisia aktoreita ovat Buzanin, Wæverin ja de Wilden mukaan ”poliittiset johtajat, viranomaistahot, hallitukset, lobbarit ja paineryhmät”.[93] Vaikkakin myöhemmät turvallistamisen teorian teoreetikot kuten Thierry Balzacq ovat esittäneet uudenlaisen viitekehyksen luomista, tässä tutkimuksessa nojataan alkuperäiseen teorian esitykseen siitä, että turvallistamisen prosessiin osallistuvat ja siten analysoinnin kohteen muodostavat yksiköt toimivat kolmella eri tasolla. Kohteen lisäksi prosessiin tarvitaan aktoreita, jotka voidaan jakaa turvallistamista tuottavien puhetekojen esittäjiin ja niitä tukeviin funktionaalisiin aktoreihin, jotka jollain tavalla ovat osa prosessin dynamiikkaa. [94]

Turvallistamisen tutkimuksessa ja turvallistamisen prosessien ymmärryksessä on Thierry Balzacqin mukaan tärkeää ennakkovaatimus tutkimuksen lähtökohdalle. Hän esittää kaksi kriteeriä, joista toisen täytyy täyttyä, jotta on ylipäätään mielekästä tutkia turvallistamista tietyssä kontekstissa.

1) Turvallistamisen kohteen tulee olla julkisen huomion tai väittelyn kohteena ja

2) tutkittavan kohteen tulee olla sellaisten lainsäädännöllisten tai poliittisten toimenpiteiden kohteena, jotka tunkevat läpi koko poliittisen systeemin.[95]

Tiedustelulaki ja siihen liittyvä julkinen keskustelu muodostavat siten erinomaisen kohteen tutkia turvallistamisen prosessia rajatussa kontektissa. Seuraavissa luvuissa esitellään lyhyesti puheaktiteoria ja turvallistamisen eri tyypit, jotka muodostavat tämä tutkimuksen metodisen viitekehyksen.

### 3.4. Puheaktit turvallistamisen teorian kiinnostuksen kohteena

Tunnetuin tapa lähestyä turvallistamista on tutkia niitä diskursseja ja erityisesti *puheakteja*, joilla turvallistaminen tapahtuu. Puheaktiteorian juuret johtavat 1960- ja 1970 -luvuille J.L. Austinin ja John Searlen teorioihin ja sääntöihin kielestä ja siihen, miten kielellä tuotetaan merkityksiä näiden sääntöjen kautta. Teorian mukaan puheaktit rakentuvat kolmesta erillisestä osasta;

[93] Buzan, Wæver ja de Wilde 1998, 40.
[94] Balzacq 2011, 35-36.
[95] Balzacq 2011, 32.

1) Lokuutio, itse lausuma eli sen foneettinen, semanttinen muoto, merkityssuhteiden joukko
2) Illokuutio, joka kuvaa puheaktin tavoitteen eli *intention,* voi olla esimerkiksi pyyntö, käsky, julistus
3) Perlokuutio, joka kuvaa *toimintaa,* sitä mitä tarkoituksella tai tahattomasti aikaansaadaan puheaktin kuulijassa, voi olla fyysistä toimintaa tai tunnetiloja. [96]

Olennaista puheaktiteoriasta peilattuna turvallistamisen teoriaan on ymmärtää se, että osa puheaktin rakenteesta, johon viitataan *illokuutiona,* voidaan katsoa olevan merkitykseltään suhteellisen pysyvä riippumatta sen puhujasta tai kontekstista kun taas *perlokuutio* eli se miten puhe tulkitaan, on aina kiinni sen kuulijasta. Turvallistamisen teorian näkökulmasta siis se mitä sanoja puheakti sisältää on vähemmän merkittävää kuin se, miten kuulija eli yleisö sanat tulkitsee. Jotta voidaan kuitenkin osoittaa turvallistamista ylipäänsä tapahtuneen, pitää siis pystyä osoittamaan että perlokuutio viesti on mennyt sen vastaanottajille perille.[97]

John Searlen ja Daniel Vandervekenin mukaan puheaktit voidaan jaotella niiden illokuutiopisteen mukaan viiteen eri tyyppiseen peruspuheaktiin.[98] Tähän on syytä tuoda mukaan myös Stephen S. Levinsonin näkökulma, jonka mukaan useampi lause yhdessä voi muodostaa yhden puheaktin vastaavasti kuin yksi lause voi sisältää monta puheaktia.[99]

**Taulukko 1. Puheaktien perusmuodot.** [100]

| Puheakti | Englanniksi | Kuvaus |
|---|---|---|
| Itsevarma | Assertive | Toteavaa, selittävää, asia on näin tyyppistä puhetta |
| Ohjaava | Directive | Sisältää pyynnön tai kehotuksen, myös suoran käskyn |
| Lupaava | Commissive | Osoittaa puhujan sitoutumista johonkin, uhkaus, lupaus |
| Kuvaileva | Expressive | Osoittaa tunteita, puheakti sisältää jonkin tunteen (anteeksipyyntö, onnittelut) |
| Julistava | Declaration | Julistavaa, puheteko itsessään saa aikaan muutoksen (esimerkkeinä käytetään tyypillisesti sodan julistusta tai aviopariksi julistamista). |

[96] Vuori 2008, 73.
[97] ma. 2008, 74.
[98] Vuori 2008, 74.
[99] Stephen C. Levinson artikkelissa Vuori 2008, 74.
[100] John Searle ja Daniel Vanderveken artikkelissa Vuori 2008, 74.

Juha A. Vuoren mukaan kompleksiset, moniosaiset puheaktit voidaan purkaa osiin käyttämällä hyväksi näitä edellä esitettyjä peruspuheakteja. Moniosaisissa puheakteissa näkyy jatkuvuus, siitä mihin yksi puheakti loppuu, seuraava alkaa.[101] Esimerkkinä kompleksisesta puheaktista Vuori käyttää narraatiota, argumentaatiota tai kuvailua ja esittää, että turvallistaminen itsessään on kompleksinen puheakti, joka voidaan myös jakaa osiin ja tunnistaa näistä osista toisistaan eroavia tapoja, erilaisia turvallistamisen puheakteja ja siten turvallistamisen eri tyyppejä.[102]

Tähän tutkimukseen Vuoren tekemä turvallistamisen tyyppijaottelu soveltuu erinomaisesti ja käytin sitä aineistoa läpikäydessä metodisena viitekehyksenä. Seuraavaksi läpikäyn tarkemmin Vuoren esittämiä turvallistamisen eri tyyppejä.

### 3.5. Turvallistamisen eri tyypit

Juha A. Vuori esittää, että turvallistamisen prosessit on mahdollista tyypitellä jakamalla niitä kuvaavat puheaktit osiin. Kaikille turvallistamistyypeille on yhteistä niiden kaksi ensimmäistä puheaktia. Ensinnäkin, ne alkavat jonkinnäköisellä *väitteellä* siitä, että jokin asia on muodostunut turvallisuuskysymykseksi, joka uhkaa olemassaoloamme. Väitteen esittäjä tekee siis kannanoton ja esittää jotakin yleisenä totuutena tavoitteenaan *vakuuttaa* yleisö turvallisuutta uhkaavasta tekijästä.[103]

Välittömästi väitteen esittämisen jälkeen, seuraa tyypillisesti *varoitus.* Jos emme reagoi jotenkin asiaan X, tapahtuu tulevaisuudessa asia Y. Puheaktina varoitus voi olla sekä *toteavaa* eli todeta tilanteen olevan näin tai *ohjaavaa* eli sisältää kehotuksen toimintaan.[104]

Varsinaiset erot turvallistamisen tyypeissä näkyvät vasta näiden kahden puheaktin jälkeen.

*Agendalle ottamisessa* väitettä ja varoitusta voi seurata erilaisia puheakteja esimerkiksi suosituksesta, kehotuksesta, pyynnöstä tai vaatimuksesta toimintaan. Tämän kolmannen

[101] Dieter Wunderlich artikkelissa Vuori 2008, 74.
[102] Vuori 2008, 75.
[103] Vuori 2008, 77.
[104] ma. 2008, 78.

puheaktin selkeänä tavoitteena on toiminnan aikaansaaminen, saada asiakysymys nostettua agendalle ja sitä kautta ehdotetut toimenpiteet toteutumaan tulevaisuudessa.[105]

*Tulevaisuuden toimenpiteiden legitimointi* on turvallistamistyypeistä kaikkein yleisin. Vuori argumentoi vahvasti sen näkemyksen puolesta, että Wæverin turvallistamisen malli kuvaa nimenomaan tätä turvallistamistyyppiä. Suurin osa turvallistamispyrkimyksistä käyttää legitimiteetin logiikkaa, mikä pyrkii legitimoimaan tulevaisuudessa vaadittuja toimenpiteitä. Tässä tapauksessa yleisön rooli on olennainen, sillä yleisö on se, joka arvioi turvallistajan, esimerkiksi poliittisten päätöksentekijöiden esityksiä ja päätöksiä. Yleisö koostuu näissä tapauksissa tyypillisesti äänestäjistä, journalisteista ja erilaisista kansalaisliikkeistä.[106] Turvallistaja pyrkii oikeuttamaan toimenpiteet, jotka normaaliolosuhteissa katsottaisiin laittomiksi tai sääntöjenvastaisiksi.

Tässä turvallistamistyypissä korostuu myös hylkäämisen mahdollisuus. Puheteko jättää tilaa ristiriidoille ja erimielisyydelle ja lopulta sille, että yleisöllä on *mahdollisuus kieltäytyä* ehdotetuista toimenpiteistä. [107] Turvallistamisen tyyppi jakaantuu kolmeen erilliseen puhetekoon 1) Asiakysymyksen nostamisena agendalle turvallisuuskysymyksenä eli väitteen esittämisenä 2) Varoituksena siitä, että jos emme tee jotain asialle X, tapahtuu tai seuraa asia Y ja 3) *Pyyntönä* siitä, että yleisö suostuu ehdotettuihin toimiin.

Pääpaino on siis sillä, että kuulijaa ei voida pakottaa hyväksymään toimenpiteitä. Päätökseen voidaan vaikuttaa argumentoimalla sen puolesta, mutta päätös ja siten turvallistaminen tapahtuu yleisön hyväksynnän kautta.[108]

Yleisön merkitys turvallistamisessa korostuu myös useiden teoreetikoiden näkökulmasta. Turvallistamisen teorian mukaan prosessilla on oltava yleisö, jolta on saatava laaja hyväksyntä ilman pakottamista. Toiset teoreetikot ovat kritisoineet alkuperäistä kööpenhaminalaisen koulukunnan teoriaa muun muassa siitä syystä, että käsitteenä yleisölle ei aseteta tarkempia

[105] ma. 2008, 78.
[106] ma. 2008, 80.
[107] Vuori 2008, 80.
[108] ma. 2008, 80-81.

kriteerejä. [109] [110] Wæverin näkemys yleisöstä pätee erityisesti sellaisissa tapauksissa, joissa yleisönä toimii asukkaat tai kansalaiset ja uhattuna on kansallinen turvallisuus. [111] Tämän tutkimuksen näkökulmasta yleisön määritelmää on syytä tarkentaa. Balzacq on omissa tutkimuksissaan nostanut esiin yleisön erilaisia rooleja, minkä päälle muun muassa Roe on rakentanut ja esittänyt, että yleisö tulisi jakaa sekä ”moraalisen tuen” antajiin ja ”muodollisen tuen” antajiin. Tämä tyypillisesti näyttäytyy siten, että moraalisen tuen ollessa riittämätöntä, viralliset tahot kuten eduskunta voi muodollisella tuellaan edustaa koko kansaa ja hyväksyä poikkeukselliset toimet konsensusperiaatteella. Tämä tukee hyvin tässä tutkimuksessa esitettyä näkemystä yleisön määrittelystä. [112]

*Uhkan tai deterrenssin käyttäminen* nähdään omana turvallistamistyyppinään. Käytettäessä deterrenssiä turvallistamistarkoituksiin viitataan silloin ehdotettujen toimenpiteiden deterrenssiin eli pelotemahdollisuuteen. Ehdotetuilla toimenpiteillä ei ole siis suoranaista vaikutusta uhan torjuntaan vaan toimenpiteiden itsessään katsotaan toimivan pelotteena ja estävän siten uhkaavia toimia.[113] Tämä turvallistamistyyppi tukeutuu siis uhkailuun ja pelotteluun ja mahdollisten toimenpiteiden uhkaan. Tämä turvallistamistyyppi edellyttää, että turvallistajana on valtio tai virallinen taho, jolla on suora vaikutusvalta turvallistettaviin ja he voivat tuoda auktoriteettiaan esiin puhetekoina. Tässä mallissa turvallistaminen kohdistetaan suoraan uhkaajiin, esimerkiksi terroristeihin, ulkomaisiin vakoojiin ja kapinallisryhmittymiin. Kolmas puheteko on tyyliltään julistava[114], asiat esitetään de facto totuuksina, mistä syystä tietyt toimenpiteet ovat perusteltuja ja välttämättömiä.[115]

*Aiempien toimenpiteiden legitimointi* fokusoituu muista turvallistamistyypeistä poiketen ajallisesti menneisyyteen tulevaisuuden sijaan. Joskus esimerkiksi on toimittu piilossa ja tehty toimenpiteitä, joita pyritään jälkikäteen legitimoimaan turvallistamalla. Aiempien toimenpiteiden legitimointi alkaa samoilla väitteen ja varoituksen puheakteilla mutta tukeutuu kolmannessa vaiheessaan siis *selitykseen.* Turvallistaminen tapahtuu siis *post hoc* tyyliin

[109] Katso esimerkiksi Sarah Leónard ja Christian Kaunert 2011, 58-59.
[110] Buzan, Wæver ja de Wilde 1998, 41. ”The audience is defined as those the securitization act attempts to convince to accept exceptional procedures because of the specific security nature of some issues”

[111] Wæver 2003, 11-12 teoksessa Balzacq 2011, 59.
[112] Sarah Leónard ja Christian Kaunert 2011, 61-62.
[113] Vuori 2008, 81.
[114] Vertaa esimerkiksi Yhdysvaltojen sota terrorismia vastaan ”War on Terrorism”.
[115] Vuori 2008, 82.

teimme asian X, jotta Y ei olisi toteutunut ja sen tavoitteena on vakuuttaa yleisö tehtyjen toimenpiteiden laillisuudesta tai tarpeellisuudesta. [116]

*Kontrollointi* on viimeinen turvallistamisen muoto. Samoin kuin deterrenssin kohdalla, myös kontrollointi edellyttää, että turvallistajana on taho, jolla on suoraa valtaa turvallistettaviin. Turvallistaminen tavoittelee siis jo olemassa olevien sääntöjen tai annettujen ohjeiden noudattamista, se voi olla yhtä hyvin jonkin tekemistä kuin jonkin tekemistä jättämistä eli kiellon noudattamista. Tämän turvallistamistyypin kolmas puheakti on jonkin asian *vaatimista.* Yleisölle ei anneta erimielisyyden mahdollisuutta, siitä syystä turvallistajalla on oltava sekä muodollinen auktoriteettiasema, että *syy* toiminnalleen. [117]

Seuraavassa taulukossa on esitetty kaikki viisi eri turvallistamisen tyyppiä ja niiden eroavaisuudet sekvenssissä, illokuutiopisteessä, perlokuution tavoitteessa, suhtautumisessa aikaan ja siihen, miten voimakkaana turvallistamisen tyyppiä voidaan pitää. Tämä puheakteihin perustuva turvallistamistyypittely muodostaa omalle tutkimukselleni metodisen viitekehyksen, jonka avulla aineistosta pyritään löytämään näitä turvallistamistyyppejä vastaavia diskursseja.

**Taulukko 2. Turvallisuustyypit (Juha A. Vuori 2008).** [118]

| **Turvallistamisen tyyppi** | **Peruspuheaktin sekvenssi** | **Illokuutio piste** | **Perlokuutio tavoite** | **Ajallisuus** | **Suhteellinen voimakkuus** |
|---|---|---|---|---|---|
| Asiakysymyksen nostaminen agendalle | 1. Esittää<br>2. Varoittaa<br>*3. Ehdottaa* | Ohjaava | Yleisön vakuuttaminen | Tulevaisuus | Tarvitsee argumentoida |
| Tulevaisuuden toimenpiteiden legitimointi | 1. Esittää<br>2. Varoittaa<br>*3. Pyytää* | Ohjaava | Legitimiteetti | Tulevaisuus | Tarvitsee argumentoida |
| Pelote / Deterrenssi | 1. Esittää<br>2. Varoittaa<br>*3. Julistaa* | Julistava | Uhkailu / pelottelu | Tulevaisuus | Julistus: vaatii muodollisen auktoriteetin |

[116] ma. 2008, 85.
[117] ma. 2008, 88.
[118] Taulukko on mukailtu ja käännetty Juha A. Vuoren artikkelista vuodelta 2008, 76. Käännökset ovat tutkijan omia.

| | | | | | |
|---|---|---|---|---|---|
| Aiempien toimenpiteiden legitimointi | 1. Esittää<br>2. Varoittaa<br>*3. Selittää* | Itsevarma | Legitimiteetti | Menneisyys | Tarvitsee argumentoida |
| Kontrolli | 1. Esittää<br>2. Varoittaa<br>*3. Vaatia* | Ohjaava | Tottelevaisuus / Kuri | Tulevaisuus | Pakottava: vaatii muodollisen auktoriteetin ja syyn |

Turvallistamisyrityksellä on aina oma vaikutuksensa eri toimijoihin, yleisöön ja näiden väliseen dynamiikkaan. Oletetaan, että normaalissa, vallitsevassa tasapainon tilassa jokin toimija esittää meitä uhkaavan asian sellaisena, että normaali, konvention mukainen toimintatapa vastata haasteeseen ei riitä ja vaatii poikkeuslupaa toimia, tai hallita toimintaansa omien intressiensä mukaisesti.[119] Tätä edeltää turvallisuusdiskurssissa asian dramatisointi tai uhkan esittäminen korkeimpana prioriteettina, jonka perusteella toimija vaatii oikeutta käsitellä asiaa poikkeuksellisin keinoin.[120]

Turvallisuus on perinteisesti ollut valtioiden välisen reaalipolitiikan ja niiden välisten voimasuhteiden diskurssia. Vasta kylmän sodan jälkeen turvallisuutta alettiin ajatella laajempana konseptina, joka kattoi sosiaalisen, poliittisen, taloudellisen ja kulttuurillisen turvallisuusulottuvuuden ulottuen siten myös inhimilliseen turvallisuuteen. [121] Aloittaako tai osoittautuuko kyberturvallisuus uuden turvallisuusparadigman aikakaudeksi, joka palauttaa valtiot turvallisuuspolitiikan keskiöön? Vai nouseeko valtioiden rinnalle turvallisuuteen keskittyviä virtuaalisia yhteisöjä, uuden digitaalisen ajan toimijoita, jotka turvaavat maailman kyberrauhaa perinteisen puolustusliiton tavoin?

### 3.6.Kyberturvallisuuden tutkimus omana sektorinaan

Kyberturvallisuuden tutkimus omana tutkimusalanaan on suhteellisen tuore vaikkakin verkottuneen teknologian riskeistä ja uhkista on käyty poliittista keskustelua 1990-luvun alusta lähtien.[122] 2010-luvulla keskustelu kyberturvallisuuden ympärillä on kiihtynyt sitä mukaa kun ymmärrys internetin merkityksestä erilaisten verkostojen, mukaan lukien terroristijärjestöjen kommunikaation mahdollistajana on lisääntynyt ja on alettu ymmärtää verkostojen merkitys ja

[119] Buzan et al. 1998, 26.
[120] Buzan et al. 1998, 26.
[121] Buzan 1983 pro gradu -tutkielmassa Juntunen, 2010, 60.
[122] Hansen & Nissenbaum 2009, 1.

kyvykkyys toimia yli valtiorajojen tai valtioita vastaan.[123] Ensimmäisenä virallisena kybersotana voidaan pitää laajamittaisia digitaalisia hyökkäyksiä Viron julkisen- ja yksityisen sektorin tahoja vastaan vuonna 2007, mikä sai myös NATO:n lisäämään ja julistamaan tietojärjestelmien turvallisuuden omalle agendalleen.[124]

Lene Hansen ja Helen Nissenbaum olivat kyberturvallisuuden tutkimuksen uranuurtajia tarttuessaan aiheeseen vuonna 2009 julkaistussa artikkelissa ”Digital Disaster, Cyber Security, and the Copenhagen School”.[125] Tutkimusartikkelissaan Hansen ja Nissenbaum tuovat hyvin esille jatketun turvallisuuden problematiikkaa ja esittävät, että normatiivisessa mielessä turvallisuuden tutkimuksessa on erittäin tärkeää ottaa huomioon laajennetun turvallisuuden käsitteet, mitkä nousevat esiin poliittisessa diskurssissa, mukaan lukien kyberturvallisuus vaikka lopputuloksena ei pystyttäisikään osoittamaan muuta kuin diskurssin ongelmallisuus. Hansenin ja Nissenbaumin tutkimuksen julkaisuun asti kyber ja turvallisuus olivat esiintyneet yhdessä turvallisuutta uhkaavana käsitteenä vain politiikassa, mediassa tai tietojärjestelmätieteiden tutkimuksessa. Tutkimuskenttänä kyberturvallisuus nähtiin haastavana, sillä sen ympärille ja siihen liittyi monia käsitteitä, jotka ovat osin päällekkäisiä kyberturvallisuuden käsitteen kanssa. Hansen ja Nissenbaum nostavat esiin joitakin tällaisia käsitteitä, kuten informaatio- tai kybersota, verkkoturvallisuus tai verkkosota, sekä esimerkiksi tietoturvallisuus.[126]

Samoin Johan Eriksson on tutkinut erilaisten IT -uhkien ja käsitteiden eroja turvallistamisen näkökulmasta. Hänen analyysinsa mukaan, se millaiseen viitekehykseen kyberuhka tai -ongelma kulloinkin liitetään, vaikuttaa siihen ketä uhkasta syytetään ja ketä pidetään vastuullisena tahona vastaamaan uhkaan. [127] Esimerkiksi hän nostaa kyberrikollisuuden ja informaatiosodankäynnin käsitteet. Kyberturvallisuutta uhkaava teko voi siis olla itsessään sama tapahtuma tai uhka, mutta se saa eri viiteyhteydessä hyvin erilaisen merkityksen. Kyberrikollisuus viittaa rikollisuuteen, mikä viittaa siihen, että syylliset ovat rikollisia ja luonnollisesti poliisi tai rikosseuraamuslaitos vastuullinen taho vastaamaan uhkaan. Jos samasta teosta puhutaan informaatiosodankäyntinä, käsitämme uhkan koskevan valtiota ja

[123] ma. 2009, 2.
[124] ma. 2009, 2.
[125] International Studies Quarterly (2009) 53, 1155 – 1175.
[126] Hansen & Nissenbaum 2009, 2.
[127] Eriksson et al. 2007, 20.

oletamme uhan tulevan toisen kansallisvaltion taholta, sekä uhkaan vastaamisen olevan valtion ja maanpuolustuksen vastuulla.[128]

Koska kyberturvallisuus muodostuu monista eri uhkatekijöistä, on kyberturvallisuudellakin useita eri turvallistamisen objekteja.[129] Ronald J. Deibert on esittänyt, että kyberturvallisuus koostuu neljästä erillisestä diskurssista, joilla jokaisella on omat objektinsa ja näitä uhkaavat tekijät sekä toimenpiteet. Hän tunnistaa erillisiksi diskursseiksi *kansallisen turvallisuuden, valtion turvallisuuden, yksilön turvallisuuden* ja neljäntenä *informaatioverkoston turvallisuuden*.[130] Digitaalisen verkoston itsessään tunnistaminen omaksi turvallisuusulottuvuudekseen kuvaa hyvin kyberturvallisuuden luonnetta. Häiriöt, katkokset, datavarkaudet tai datan korruptoituminen informaatioverkossa tekevät verkosta itsessään sekä turvallisuuden kohteen, että turvallisuutta uhkaavan tekijän. Deibert itse asiassa väittääkin, että sitä mukaa kun olemassaolomme ja elämämme siirtyy verkkoon tai perustuu verkon päälle rakennettaviin sovelluksiin, neljännestä turvallistamisen objektista tulee primääriobjekti, jonka perustaan muiden turvallistamisobjektien olemassaolo perustuu.[131]

Hansenin ja Nissenbaumin tutkimusartikkelin tarkoitus oli siten kuroa kiinni puutteellisen kyberturvallisuustutkimuksen vajetta. Tutkimuksen lähtökohtana toimii turvallisuudentutkimuksen kööpenhaminalainen koulukunta, joka tutkii turvallisuutta ennen kaikkea puheakteina, mikä pyrkii turvallistamaan erilaisia kohteita eli objekteja[132]. [133] Historiallisesti tällaisina turvallistamisen objekteina ovat toimineet valtio tai kansakunta, joiden fyysistä tai ideologista turvallisuutta jokin taho uhkaa siten, että objektin voidaan katsoa vaativan erityistä ja välitöntä suojelua. [134]

Erittäin mielenkiintoisena näkökulmana artikkelissa esitetään se, että kööpenhaminalainen koulukunta vuonna 1998 katsoo kyberturvallisuuden turvallistamisyritykseksi mutta ei näe perusteita sille, että kyberturvallisuus teoretisoitaisiin omaksi erilliseksi alueekseen samoin

[128] mt. 2007, 20.
[129] Lobato et al. 2015, 26.
[130] Deibert (2002) Hansen & Nissenbaumin artikkelissa 2009, 1163.
[131] Lobato et al. 2015, 26.
[132] Eng. referent object.
[133] Hansen & Nissenbaum 2009, 2.
[134] ma. 2009, 1156.

kuin sotilaallinen-, poliittinen-, yhteiskunnallinen-, ympäristö-, taloudellinen- tai uskonnollinen turvallisuus.[135]

Buzan, Wæver ja de Wilde perustelivat tätä Pentagonin esimerkillä. Pentagon esitti jo vuonna 1996, että ”hakkerit muodostavat katastrofaalisen uhan” ja ovat ”vakava uhka kansalliselle turvallisuudelle” mutta Buzan, Wæver ja de Wilde katsoivat kyseessä olevan turvallistamisyritys, sillä vaikka diskurssi ja retoriikka saattaisivat johtaa toimenpiteisiin tietojärjestelmäturvallisuudessa, niillä ei katsottu olevan laajempia vaikutuksia muihin turvallisuuskysymyksiin.[136] [137]

Hansen ja Nissenbaum esittävät kuitenkin omassa tutkimusartikkelissaan, että kyberturvallisuus itse asiassa on jo virallisesti turvallistettua, mikä ilmenee valtiollisten toimijoiden julkilausumina tai kyberturvallisuusstrategioiden tuottamisena. [138] Tässä on kuitenkin suuria eroja riippuen siitä, missä kontekstissa kyberturvallisuutta tarkastellaan. Eri maissa informaatioteknologinen infrastruktuuri on hyvin eri tasoilla, eikä siten voida esittää, että kyberturvallisuus olisi universaalisti turvallistettua. Omassa tutkimuksessani tutkimuksen lähtökohdaksi asetetaan se, että kyberturvallisuus käsitteenä turvallistetaan eri maissa sitä mukaa kun nämä saavuttavat tietyn teknisen kypsyystason. Turvallistamisen prosessi etenee vaiheittain ja näyttäytyy eri tavoin riippuen siitä missä sitä tarkastellaan. Erilaisten tapaustutkimusten kautta on siten mahdollista oppia ymmärtämään turvallistamisen prosessia ja kyberturvallisuutta ilmiönä.

Tästä osoituksena on viime vuosilta löytämäni muutamat tutkimusartikkelit, missä läpikäydään kyberturvallisuuden turvallistamisprosessia eri valtioita ja niiden kyberturvallisuusdiskurssia esimerkkeinä käyttäen. Osa tutkimusartikkeleista keskittyi yhden valtion tapaustutkimukseen[139], toiset vertailivat kyberturvallisuusdiskursseja eri valtioiden välillä.[140]

[135] ma. 2009, 1156.
[136] ma. 2009, 1156.
[137] Buzan et al. 1998, 25.
[138] Hansen & Nissenbaum 2009, 1157.
[139] Ks. esimerkiksi Estonian tapaus Hansen & Nissenbaumin artikkelissa 2009.
[140] Ks. esimerkiksi vertaileva tutkimus Brasilian ja Yhdysvaltojen kyberturvallisuusdiskurssista Lobato & Kenkel artikkelissa 2015.

### 3.7.Kyberturvallisuuden kolme turvallistamisen diskurssia

Kyberturvallisuuden diskurssi liikkuu suvereenisti yli sellaisten rajojen, joita perinteisesti pidetään turvallisuudentutkimuksessa annettuina. Näitä ovat rajat yksityisen ja kollektiivisen turvallisuuden välillä, sekä rajat julkisten ja yksityisten toimijoiden ja taloudellisen ja poliittisen sekä sotilaallisen turvallisuuden välillä. Kuten aiemmin on jo todettu, kyberturvallisuus ei tunnusta rajoja; samat informaatioverkon kiristys- tai haittaohjelmat uhkaavat yhtälailla yksityistä taloudellista sektoria kuin julkista, kansallista sektoria.[141] Hansen ja Nisseubaum (2009) tunnistavat monia samankaltaisuuksia kybertoimintaympäristön ja esimerkiksi taloudellisen toimintaympäristön välillä, molemmat liikkuvat joustavasti yli kansallisvaltioiden rajojen ja auktoriteetti ja suvereniteetti on hajautunutta. Toimintaympäristö muodostaa kompleksisen systeemin, missä turvallistettavia objekteja on samanaikaisesti useita läsnä. Samoin uhkan lähdettä tai hyökkääjän alkuperää on usein vaikea tunnistaa.[142] Vaikka kyberturvallisuusympäristö peilaa monilta osin taloudellista ympäristöämme, ei se kuitenkaan rajoitu siihen, mikä tuo sen Hansenin ja Nissenbaumin näkemyksen mukaan lähemmäs kansallista ja sotilaallista turvallisuutta.[143]

Hansen ja Nissenbaum argumentoivat, että perinteisesti kyberturvallisuusdiskurssi on yrittänyt pitää kiinni julkisen ja yksityisen sektorin sekä yksityisen ja valtion vastakkainasettelusta. Esimerkkeinä he nostavat muun muassa yksityisyyden suojan loukkaamiset ja informaation vapaan kulun valtiorajojen yli uhkana valtiolle ja kansalliselle identiteetille.[144] [145]

Kööpenhaminalaiselle koulukunnalle on tunnusomaista luoda jokaiselle turvallisuussektorille oma *kieliopillinen* tapa sitoa turvallistamisen objektit, uhat ja turvallistavat aktorit omiksi *konsepteikseen*. Samaan tapaan Hansen ja Nisseubaum ovat esittäneet oman teoreettisen näkemyksensä kyberturvallisuussektorin diskursiivisista konsepteista.[146] Allaolevassa taulukossa esitellään nämä konseptit ja niiden kuvaukset:

[141] Hansen & Nissenbaum 2009, 1161.
[142] ma. 2009, 1162.
[143] ma. 2009, 1162.
[144] Vertaa esim. Kiinan internetsensuuri.
[145] Hansen & Nissenbaum 2009, 1162.
[146] ma. 2009, 1163-1164.

**Taulukko 3. Kyberturvallisuuden diskursiiviset konseptit.**[147]

| Turvallistamisen konsepti | Englanniksi | Kuvaus |
|---|---|---|
| Hyperturvallistaminen | Hypersecuritization | Turvallistamisen äärimmäinen muoto. Turvallisuusuhkan liioittelu ja/tai vastaavasti uhkaan vastaamisen toimenpiteiden ylimitoittaminen. Vertauksena kielikuvat esimerkiksi *ydintuhosta* tai *elektronisesta Pearl Harborista*. |
| Arkipäiväiset turvallisuusteot | Everyday Security Practice | Arkipäiväisillä turvallisuusteoilla viitataan jokapäiväiseen virtuaalimaailman turvallisuuteen esimerkiksi suojautumalla tietokoneviruksilta. Merkittävää tässä diskurssissa on yksilön merkitys sekä uhkan kohteena, että uhkana järjestelmän näkökulmasta. |
| Teknillistäminen | Technification | Informaatiotieteiden teknisen luonteen vuoksi niiden ymmärtäminen vaatii teknistä ymmärrystä, mikä puolestaan luo tilauksen erityisosaamiselle ja asiantuntijadiskurssille. Kyberturvallisuussektorille on ominaista, että poliitikot ja media tukeutuvat asiantuntijoihin turvallistamisen yrityksissään. |

Kyberturvallisuuden diskurssille on ominaista se, että samaan aikaan esiintyy useita eri diskursseja yhteenliitettyinä toisiinsa.[148] Tämän tutkimuksen näkökulmasta on siis hyvä huomioida ennen siirtymistä aineiston analysointiosuuteen, että peilatessa kyberturvallisuutta turvallistamisen teoriaan, on oletettavissa että turvallisuuspuheesta nousee esiin useita, samanaikaisesti vaikuttavia diskursseja, jotka kilpailevat keskenään.

[147] Hansen & Nissenbaum 2009, 1163-1167. Katso myös Kenkel et al. 2015, 31.
[148] Kenkel et al. 2015, 32.

# 4. ANALYYSIOSIO

## 4.1. Suomen kyberturvallisuusstrategia – lyhyt evoluutio

Suomella on ollut virallinen kyberturvallisuusstrategia vuodesta 2013 lähtien. Tämän tutkimuksen toteuttamiseen mennessä strategiaa on viety käytäntöön toimeenpano-ohjelmin hieman yli viisi vuotta. Käsityksemme ja kokemuksemme tästä uudesta turvallisuuden alasta voidaan siis katsoa olevan verrattain rajalliset. Ymmärrämme kuitenkin, että Suomi on edistynyt tietoyhteiskunta, minkä toiminta perustuu erilaisten tietoverkkojen ja -järjestelmien toimivuuteen sekä kansallisella, että globaalilla tasolla. Nämä järjestelmät, joita käyttävät valtion ja yhteiskunnan lisäksi yksityisen sektorin toimijat muodostavat monimutkaisen keskinäisriippuvuussuhteen, mikä kuvaa hyvin vallitsevaa kybertoimintaympäristöä. [149] [150]

Kyberturvallisuusstrategian lähtökohta on, että tämä keskinäisen riippuvuuden suhde tekee järjestelmästä *erityisen haavoittuvan*[151] mistä syystä valtiolla on voimakas intressi pyrkiä turvaamaan sen toimintaa. Tietojärjestelmiin linkittynyt toiminta nähdään kriittisenä ja elintärkeänä ja digitaalisesta verkostosta itsessään on tullut monessa mielessä yhteiskunnallisen toiminnan perusta.[152]

Toisaalta kybertoimintaympäristö nähdään myös mahdollisuutena ja voimavarana. Jos pystymme turvaamaan ja varmistamaan kybertoimintaympäristön toimivuuden, katsotaan sen helpottavan yksilöiden ja yritysten toimintaa ja sitä kautta taloudellista aktiviteettia. Siten toimintaympäristöstä itsessään tulee kilpailuetu, mikä parantaa osaltaan myös Suomen houkuttelevuutta kansainvälisenä investointikohteena. Myös kyberturvallisuuden rooli itsessään uutena ja kasvavana liiketoiminta-alueena tunnistetaan.[153] [154] Keskinäisriippuvuuden merkitys korostuu, *kansallinen kyberturvallisuus ja suomalaisten yritysten menestys ovat yhteydessä keskenään.*[155] Myös vuonna 2016 julkaistun liikenne- ja viestintäministeriön

[149] Suomen kyberturvallisuusstrategia 2013, 1.
[150] Suomen kyberturvallisuusstrategia 2013, 1. Yhteiskunnan lisääntynyt tietointensiivisyys, ulkomaisen omistuksen kasvu ja toimintojen ulkoistaminen, tieto- ja viestintäjärjestelmien keskinäinen integraatio, kaikille avointen tietoverkkojen käyttö sekä lisääntynyt riippuvuus sähköstä ovat asettaneet uudenlaisia vaatimuksia yhteiskunnan elintärkeiden toimintojen turvaamiseksi normaalioloissa, normaaliolojen vakavissa häiriötilanteissa ja poikkeusoloissa.
[151] Suomen kyberturvallisuusstrategia 2013, 1.
[152] Katso myös Deibertin käsitys digitaalisen verkostosta neljäntenä turvallisuusulottuvuutena
[153] Suomen kyberturvallisuusstrategia 2013, 1.
[154] Turvallisuuskomitea 2014
[155] Suomen kyberturvallisuusstrategia 2013, 1.

tietoturvallisuusstrategian visiona on, että *maailman luotetuin digitaalinen liiketoiminta tulee Suomesta* [156].

Suomen kyberturvallisuusstrategia määrittelee keskeiset tavoitteet ja toimintalinjat, joilla toimintaympäristön turvallisuus ja toimivuus varmistetaan.[157] Strategian alkuperäinen visio kuvattiin vuonna 2013 seuraavasti:

• *Suomi kykenee suojaamaan elintärkeät toimintonsa kaikissa tilanteissa kyberuhkaa vastaan.*

• *Kansalaisilla, viranomaisilla ja yrityksillä on mahdollisuus tehokkaasti hyödyntää turvallista kybertoimintaympäristöä ja sen suojaamiseen syntyvää osaamista sekä kansallisesti että kansainvälisesti.*

• *Vuonna 2016 Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa.*[158] [159]

Keskeinen osa kyberturvallisuusstrategian toteutumisen varmistamista oli erikseen laadittava ja toteutettava toimeenpano-ohjelma, johon kirjattiin yhteensä 74 toimenpidettä. Keskeisessä roolissa toteutettavissa toimenpiteissä olivat muun muassa kyberturvallisuuskeskuksen perustaminen, valtion ympärivuorokautisen tietoturvatoiminnan varmistaminen, poliisin toimintakyvyn varmistaminen *"..kyberrikollisuuden torjunnassa, kybertoimintaympäristöön ja kyberturvallisuuteen liittyvän lainsäädännön kehittäminen.."* ja alueeseen liittyvän *"..osaamisen vahvistaminen.."* koulutuksen ja tutkimusohjelmien kautta.[160] [161]

---

[156] Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017 – 2020, 2017, 5. Suomella nähdään olevan hyvät edellytykset tulla tunnetuksi osaavana, menestyvänä ja luotettavana maana, jossa on turvallista tarttua digitalisaation mukanaan tuomiin mahdollisuuksiin. Talouskasvun luominen ja kiihdyttäminen riippuu siitä, että kehitämme, omaksumme ja kokeilemme uudenlaisia, digitaalisen tiedon hyödyntämiseen perustuvia liiketoiminnan ja ansainnan malleja. Tämän edellytyksenä on arvioitu tarvittavan luottamusta uusiin palveluihin, liiketoimintamalleihin ja markkinatoimijoihin sekä vahvaa otetta tietoturvallisuuden osaamisesta ja markkinoiden kehittämisestä.

[157] Suomen kyberturvallisuusstrategia 2013, 1.

[158] Suomen kyberturvallisuusstrategia 2013, 3.

[159] Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017 – 2020, 2017, 7. Vuonna 2017 julkaistun päivitetyn toimeenpano-ohjelman myötä vision kolmannen kohdan osalta vuoteen 2016 sidottu tavoite muutettiin pysyväksi:" Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa".

[160] Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2014, 2.

[161] Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017 – 2020, 2017, 4. Suomen ensimmäinen kansallinen kyberturvallisuusstrategia julkaistiin valtioneuvoston periaatepäätöksenä 24.1.2013. Siinä määriteltiin ne "..tavoitteet ja toimintalinjat, joiden avulla vastataan kybertoimintaympäristöön kohdistuviin haasteisiin ja varmistetaan sen toimivuus". Strategiassa kuvattiin kyberturvallisuuden visio ja strategiset linjaukset sekä todettiin, että strategisten linjausten toteuttamiseksi ja vision kuvaamaan tavoitetilaan pääsemiseksi laaditaan toimeenpano-ohjelma. Turvallisuuskomitea hyväksyi strategian ensimmäisen toimeenpano-ohjelman 11.3.2014 ja on säännöllisesti arvioinut toimeenpano-ohjelman toteutumista.

Vuoteen 2017 mennessä käsitys kyberturvallisuudesta keskinäisriippuvuussuhteena valtion, julkisten ja yksityisten yhteiskunnallisten toimijoiden välillä on voimistunut. Elinkeinoelämän toimijoiden merkitys sekä kansallisissa, että kansainvälisissä palvelukokonaisuuksissa ja -verkostoissa korostuu. Toimeenpano-ohjelman johdannossa todetaankin seuraavasti:

*Kyberturvallisuusstrategian julkaisun jälkeen kyberturvallisuuden toimintaympäristö on muuttunut uusien palvelutuotantomallien, teknologioiden ja niihin kohdistuvien uusien uhkien myötä.*[162]

Uuden toimeenpano-ohjelman pohjalla on valtioneuvoston helmikuussa 2017 julkaisema selvitys ”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi”.[163] Tuoreempi toimeenpano-ohjelma ottaa myös selkeämmin kantaa digitalisaatioon ja siihen liittyviin teemoihin kuten tiedolla johtamiseen, tekoälyyn, robotisaatioon tai esineiden internetin myötä lisääntyviin kyberturvallisuuden tarpeisiin ja niiden merkityksen kasvuun. Samaa tahtia teknologian edistymisen ja palveluiden lisääntymisen myötä yhteiskunnan elintärkeiden toimintojen turvaaminen sekä kansallisessa, että kansainvälisessä toimintaympäristössä koetaan yhä keskeisemmäksi.[164]

Vuoden 2017 – 2020 toimeenpano-ohjelmassa korostuu myös kaksi merkittävää asiaa, kansallisen turvallisuuden painottaminen ja muutoksen korostaminen. Myös valtioneuvoston puolustusselonteko keväältä 2017 painottaa kybertoimintaympäristön merkityksen kasvua.

*Kybertoimintaympäristön merkitys kasvaa. Kyberkeinojen käyttöä poliittisten päämäärien saavuttamiseksi ei voida sulkea pois. Yhteiskunnan digitalisaatio, teknisten järjestelmien riippuvaisuus rajat ylittävistä tietoverkoista sekä järjestelmien keskinäiset riippuvuussuhteet ja haavoittuvuudet altistavat yhteiskunnan elintärkeät toiminnot kybervaikuttamiselle. Kyber- ja informaatiovaikuttamista on kohdistettu lähialueillemme ja myös Suomeen mm. kriittistä infrastruktuuria, teollisuuslaitoksia sekä poliittista päätöksentekojärjestelmää ja kansalaisia vastaan. Tieteen ja teknologian kehitys aiheuttaa myös muunlaisia haasteita uhkiin varautumiselle.*[165]

Vain muutamassa vuodessa kybertoimintaympäristön koetaan muuttuneen niin voimakkaasti, että se vaatii valtiolta erityisiä toimenpiteitä kansallisen turvallisuuden säilyttämiseksi.

[162] Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017 – 2020, 2017, 4.
[163] Valtioneuvosto 17.2.2017 ”Tutkimushankkeessa tehtiin analyysi kyberturvallisuuden megatrendeistä, selvitettiin kyberturvallisuuden nykytilaa ja kehittämistarpeita julkisella ja yksityisellä sektorilla, analysoitiin kuuden maan (Alankomaat, Iso-Britannia, Israel, Ruotsi, Singapore ja Viro) kyberturvallisuuden nykytilaa ja sen kehittämistä. Tutkimuksen yhteenvetona esitetään tunnistetut puutteet ja kehityskohteet kyberturvallisuuden tavoitetilan 2020 saavuttamiseksi”.

[164] Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017 – 2020, 2017, 5.
[165] Valtioneuvoston puolustusselonteko 2017, 9.

Seuraavassa luvussa siirrymme tarkastelemaan tapaustutkimuksen kohdetta, Suomen tiedustelulainsäädännön uudistusta.

## 4.2. Case Tiedustelulaki

Laadullisessa tutkimuksessa korostuu sen ymmärtäminen, tutkitaanko ilmiöön liittyviä käsityksiä vai kokemuksia. On tärkeää ymmärtää tutkimuksen konteksti eli se millaiseen toimintaympäristöön tutkimus nojaa ja millaisia erilaisia sosiaalisia, historiallisia tai kulttuurillisia olettamuksia on läsnä tutkimusta tehdessä. [166] Samoin muistetaan se, että käsitykset ja kokemukset eivät välttämättä vastaa toisiaan. Buzanin mukaan turvallistamisen näkökulmasta ei ole merkitystä sillä onko kokemamme uhka todellinen vai kuviteltu, riittää että käsityksemme siitä on todellinen. [167]

Kontekstin lisäksi tärkeitä elementtejä tässä tutkimuksessa on myös *intentio* eli turvallistamisen teorian näkökulmasta puheaktorin motiivit ja *prosessi* eli tämän tutkimuksen näkökulmasta se, miten diskurssien ja puheaktien avulla tiedustelulainsäädännöstä käytävää keskustelua pyritään turvallistamaan.[168]

Tapaustutkimus muodostaa usein turvallistamisen tutkimuksen rungon, niin myös tässä tutkimuksessa. Se on empiiristä tutkimusta, jonka tavoitteena on tutkia ja ymmärtää jotakin ilmiötä syvällisesti sen todellisessa ympäristössä. Turvallistamisen teorian kontekstissa tapaustutkimukset voidaan jaotella tyypillisiin, kriittisiin ja paljastaviin tutkimustyyppeihin. Siinä missä kriittinen tapaustutkimus pyrkii tuomaan jotakin uutta turvallistamisen teoriaan ja paljastava tutkimus nostamaan esiin jotakin sellaista mitä sosiaalisesta ilmiöstä ei ole aiemmin tiedetty, ei tyypillinen tapaustutkimus pyri testaamaan teoriaa tai rakentamaan sen päälle, vaan sen tarkoitus on ennemminkin selittää turvallistamisen prosessia tai logiikkaa tietyn tapauksen valossa. [169]

Balzacq nostaa esiin myös olennaisen haasteen, joka liittyy tapaustutkimuksen käyttämiseen turvallisuuden tutkimuksessa. Monet alan teoreetikot, kuten Buzan, Wæver ja De Wilde lähtevät siitä ajatuksesta, että turvallistamista voidaan tutkia vain sellaisten turvallistamisyritysten kautta, joiden lopputulos on positiivinen. Tämä saattaa johtaa siihen, että

[166] Vilkka 2015, 75-76.
[167] Buzan et al. 1998, 24.
[168] Vilkka 2015, 76-77.
[169] Balzacq 2011, 34.

teorian testaamisen sijaan valitaan vain tapaustutkimuksia, joilla voidaan vahvistaa jo olemassaolevaa käsitystä ja näin epähuomiossa tulla ylikorostaneeksi tiettyjä syy-seuraussuhteita. Tärkeää turvallisuudentutkimuksessa, samoin kuin tässä tutkimuksessa on säilyttää koko ajan tietoisuus analyyttisestä viitekehyksestä ja on syytä olla yleistämättä tutkimuksen lopputuloksia.[170]

Balzacq muistuttaa, että vaikka tiedämme, mikä ongelma on, emme sen perusteella pysty vielä päättelemään, mikä tekee siitä ongelman, miksi, kenelle ja miksi juuri nyt? [171]

Suomessa kyberturvallisuuskeskustelu on viimeisen kahden vuoden aikana kulminoitunut uuteen tiedustelulainsäädäntöön. Voimakas vastakkainasettelu yksilönsuojan ja viestisalaisuuden loukkaamattomuuden ja toisaalta kansallisen turvallisuuden välillä on saanut erittäin suuret mittasuhteet – tästä kertoo erityisesti se, että lainsäädäntöä on pyritty kiirehtimään jopa perustuslain säätämistä kiireellisellä lainsäädäntöjärjestyksellä. Seuraavissa alaluvuissa käsitellään tiedustelulainsäädäntöprosessin etenemistä kronologisessa järjestyksessä peilaten samalla aineistoa Juha A. Vuoren eri turvallistamisen tyyppeihin.

### 4.2.1. Kyberturvallisuus nousee agendalle

Turvallistaminen on ensisijaisesti prosessi, joka etenee sen lähtökohdasta eli turvallistamisen kohteen eli asiakysymyksen nostamisesta agendalle vaiheittain kohti onnistuneesti turvallistettua tilannetta. Silloin kun jokin asiakysymys nousee agendalle eli *politisoituu* turvallisuuskysymyksenä, on turvallistaminen vielä melko ehdollista. Usein tällaisten asiakysymysten nousu julkiseen keskusteluun tapahtuu yksittäisten poliitikoiden, tutkijoiden tai journalistien toimesta mutta tavoite on kuitenkin selkeästi toiminnallinen, asiakysymyksestä pyritään tekemään turvallisuuskysymys, jotta sillä voidaan perustella mahdollisia toimenpiteitä, joita turvallistaja ajaa tai ehdottaa kyseiseen uhkaan vastaamiseksi.[172]

Tiedustelulainsäädännön muutoksen siemenet kylvettiin marraskuussa 2013. Puolustusministeriö oli kyberstrategian mukaisesti tarkastellut Suomen lainsäädäntöä ja sen riittävyyttä ja verrannut Suomen lainsäädäntöä useisiin eri maihin. Puolustusministeriön selvityksen mukaan useissa maissa kybertoimintaympäristön nopeaan kehittymiseen ja muuttumiseen oli vastattu uudistamalla kansallista lainsäädäntöä erityisesti koskien valtion

[170] mt. 2011, 34.
[171] mt. 2011, 32.
[172] Vuori 2008, 77.

turvallisuusviranomaisten tiedonhankintaa. Kyberturvallisuusstrategian toimeenpano-ohjelman mukaisesti asiaa selvittämään asetettiin puolustusministeriön työryhmä, jonka tehtävänä oli *selvittää turvallisuusviranomaisten tiedonhankintaa koskevat toimintaedellytykset, erityisesti kybertoimintaympäristön kautta Suomeen kohdistuvat uhkat ottaen huomioon sekä tiedonhankintaa koskevat nykyiset toimivaltuudet että niiden kehittämistarpeet.* Toimeenpano-ohjelmassa korostettiin, että on *..tärkeää ottaa huomioon myös yksilön oikeusturva sekä tehokkaat perustuslailliset valvontamekanismit.* [173]

Alkuperäisessä kyberturvallisuusstrategiassa turvallisuusdiskurssissa painottuu yhteiskuntajärjestys ja kyberturvallisuus nähdään ensisijaisesti varautumisena verkossa tapahtuvaan rikolliseen toimintaan:

*...varmistetaan, että poliisilla on riittävä toimivalta sekä osaaminen ja riittävät tiedonsaantioikeudet tunnistaa ja torjua tietoverkossa tapahtuva terroristien ja muiden yhteiskuntajärjestystä vaarantavien rikosten valmistelu, rahoitus, johtaminen ja niihin liittyvä propagandistinen tiedottaminen ja mielipiteenmuokkaus sekä kyky selvittää epäillyt rikokset.*[174]

Strategiadokumentti käsittelee kyberturvallisuutta koko yhteiskuntaan vaikuttavana, mutta kansalliseen turvallisuuteen viitataan ainoastaan kansallisen *kyberturvallisuuden* kautta. Tämä on tulkittavissa siten, että kyberturvallisuus nähdään vielä erillisenä turvallisuuden ulottuvuutena.

Lokakuussa 2015 Sisäministeriö tiedotti hallituksen esityksestä uudistaa Suomen tiedustelulainsäädäntö. Kolmen erillisen lainsäädäntöhankkeen tavoitteiksi esitettiin Suomen kansallisen turvallisuuden ja kansainvälisistä sotilaallisista uhista saatavan tiedon parantaminen. Samalla kerrottiin, että luottamuksellisen viestin suojaa koskeva mahdollinen perustuslain muutos tullaan selvittämään. Suurimmaksi ongelmakohdaksi voimassaolevassa perustuslaissa katsottiin se, että nykyinen perustuslaki ei tunnusta viestin suojan rajoittamista kansallisen turvallisuuden suojaamiseksi. [175] Enää ei siis puhuttu kansallisesta *kyber*turvallisuudesta, nyt puhuttiin *kansallisesta* turvallisuudesta.

[173] Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2013, 12.
[174] Suomen kyberturvallisuusstrategia 2013, 27.
[175] Sisäministeriön tiedote 1.10.2015. ”Perustuslain nykyisen sanamuodon mukaan lailla voidaan säätää välttämättömistä rajoituksista kirjeen, puhelun ja muun luottamuksellisen viestin salaisuuteen vain yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapaudenmenetyksen aikana. Lailla ei siten voida säätää viestin suojan rajoittamisesta muissa tarkoituksissa, kuten esimerkiksi kansallisen turvallisuuden suojaamiseksi”.

### 4.2.2. Kansallinen turvallisuus vaikuttavana diskurssina

Tiedustelulakitapauksessa on merkittävää, että sen alkumetreiltä lähtien *kansallinen turvallisuus* on nostettu esiin turvallistamisen kohteena. Muutos ei ole merkittävä vain lainsäädännöllisellä tasolla vaan myös retorisella tasolla. ”Aiemmin Supon tiedustelullista tehtävää on ensisijassa tarkasteltu ja ohjattu rikostorjunnan eikä kansallisen turvallisuuden näkökulmasta.”[176] Oletus ja ajatus siitä, että kyberuhkat ovat siirtyneet tietoturvarikoksien tasolta kansallista turvallisuutta ja siten koko olemassaoloamme uhkaaviksi toimiksi on merkittävä diskurssin muutos.

*Kansallista turvallisuutta vakavasti uhkaavalla toiminnalla tarkoitettaisiin säännöksessä kansanvaltaista valtio- ja yhteiskuntajärjestystä, yhteiskunnan perustoimintoja, suuren ihmismäärän henkeä tai terveyttä tai kansainvälistä rauhaa ja turvallisuutta uhkaavaa toimintaa. Edellytyksenä olisi kuitenkin se, että toiminnalla olisi jokin kytkentä Suomeen ja että se uhkaisi nimenomaan Suomen kansallista turvallisuutta.*[177]

Turvallistamisen prosessin näkökulmasta tämä on ensimmäinen askel. Buzan, Wæver ja de Wilde ovat esittäneet, että jotta turvallistamista voidaan katsoa ylipäätään tapahtuneen, pitää uhattuna olla jokin rajattua joukkoa suurempi kokonaisuus ja sen koko olemassaolo, puhutaan siis eksistentiaalisesta uhasta.[178]

*Kyberhyökkäyksillä voidaan tuottaa suuria häiriöitä ja jopa lamauttaa osia kriittisestä infrastruktuurista ja yhteiskunnan elintärkeistä toiminnoista. Valtio tai organisaatio voidaan painostaa poliittisiin, sotilaallisiin tai taloudellisiin myönnytyksiin.* [179]

Perinteisestä turvallistamisen teorian näkökulmasta sekä valtio ja sen kansalaiset eli kansallinen turvallisuus ovat kohteena ja siten turvallistamisen objekteina. Valtion asemaa korostetaan, sekä toimijana, että kohteena. Samoin aineistosta nousee esiin myös tietoverkoston rooli kriittisen inftrastruktuurin ylläpitäjänä ja siten sen rooli myös uhkan kohteena.[180]

*Suomen turvallisuusympäristö on muuttunut nopeasti johtuen muun muassa globalisoitumisesta ja digitalisaation kehityksestä. Turvallisuus- ja toimintaympäristön muutosten myötä kansallisen turvallisuuden uhat, kuten vakoiluun ja terrorismiin liittyvät ilmiöt ja hankkeet, siirtyvät yhä enemmän verkkoon. Muutoksiin vastaaminen edellyttää lainsäädännön tarkistamista niin, että kansallisesta turvallisuudesta vastaavat viranomaiset pystyvät hoitamaan lakisääteiset tehtävänsä riittävän tehokkaasti.*[181]

[176] Sisäministeriön uutinen 10.11.2016.
[177] Oikeusministeriön tiedote 25.1.2018.
[178] Buzan et al. 1998, 24-25.
[179] Deibert 2002 artikkelissa Kenkel & Lobato 2015.
[180] Deibert 2002 artikkelissa Kenkel-Lobato 2015.
[181] Sisäministeriön tiedote 1.10.2015.

Kansalliseen turvallisuuteen kohdistuvan uhan koetaan tulevan ulkomailta erityisesti globalisaatiosta ja digitalisaatiosta johtuen. [182] Vakoiluun ja terrorismiin liittyvät ilmiöt liitetään yhä useammin tietoverkkoihin, millä perustellaan muutosta tiedustelulakiin ja viranomaisvaltuuksien lisäämistä verkkotiedusteluun. [183]

Aktoreina eli turvallistajina kyberturvallisuuden agendalle nostamisessa ovat ensisijaisesti tiedusteluviranomaiset eli puolustusvoimien ja suojelupoliisin edustajat. Puheakti näyttäytyy väitteinä, vakuutteluna ja todisteluina.[184] Tavoitteena on siis aikaansaada kuulijassa hyväksyntä sille, että kansallisen turvallisuutemme tilanne on muuttunut. Läsnä turvallistamispuheessa on useita emootioita herättäviä diskursseja kuten ’*kansallinen turvallisuus*’, ’*terrorismi*’ ja ’*vakoilu*’.

Tätä seuraa varoitus. Jos emme ryhdy toimenpiteisiin välittömästi, meitä uhkaa jokin asia X[185]

*Sisäministeriön hanke keskittyy siviilitiedustelua koskevan lainsäädännön valmisteluun. Hankkeen keskeisin tavoite on kansallisen turvallisuuden parantaminen. Tavoitteena on parantaa turvallisuusviranomaisten kykyä ennakoida ja estää toimialallaan sellaisia vahingollisia tekoja ja toimenpiteitä, jotka voivat vaarantaa erityisen tärkeiksi miellettyjä kansallisia etuja.[186]*

Ja lopulta suositus, ohjaava puheteko, jolla pyritään vaikuttamaan siihen miten uhkaan pitäisi varautua. [187]

*Oikeusministeriön asettama asiantuntijatyöryhmä selvittää perustuslain tarkistamista siten, että lailla voitaisiin säätää tarpeellisiksi katsottavien edellytysten täyttyessä kansallisen turvallisuuden suojaamiseksi välttämättömistä rajoituksista luottamuksellisen viestin salaisuuden suojaan.[188]*

Tässä sisäministeriön tiedotteessa on nähtävissä selkeästi turvallistamisen elementtejä, jotka sopivat turvallistamistyypiltään asiakysymyksen agendalle nostamiseen. [189] Oman tulkintani mukaan tässä kohtaa turvallistettava yleisö ei ole vielä koko kansa vaan turvallistamispuhe on suunnattu niille parlamentaarisille tahoille, jotka käynnistävät tai ovat mukana uuden tiedustelulainsäädännön valmistelussa.

Turvallistamisen prosessin voidaan siis katsoa käynnistyneen virallisesti sisäministeriön tiedottaessa tiedustelulainsäädännön uudistamiseksi käynnistettävistä toimenpiteistä.

[182] Sisäministeriön tiedote 19.4.2017.
[183] Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017 – 2020, 2017, 6.
[184] Vuori 2008, 77.
[185] ma. 2008, 78.
[186] Sisäministeriön tiedote 1.10.2015.
[187] Vuori 2008, 78.
[188] Sisäministeriön tiedote 1.10.2015.
[189] Sisäministeriön tiedote 1.10.2015.

Seuraavassa luvussa pureudutaan tarkemmin turvallistamisen teorian näkökulmasta turvallistamisprosessin välttämättömiin elementteihin, nimenomaisesti laajan yleisön hyväksyntään ja *tulevaisuuden toimien legitimoinnin* turvallistamistyyppiin.

### 4.2.3. Tiedustelulain legitimointi

Turvallistamisen teoria pyrkii selittämään ja ymmärtämään turvallisuutta ilmiönä sen kautta millaisista kysymyksistä tehdään turvallisuuskysymyksiä, kenen toimesta, kuka on kohdeyleisö ja erityisesti siitä, miten turvallistaminen tapahtuu, millaisin seurauksin ja minkälaisissa toimintaympäristöissä.[190] Kontekstilla on siis merkitystä. Kun turvallistamisen prosessi tulee läpinäkyvämmäksi, voimme vaikuttaa siihen. Demokraattinen päätöksentekoprosessi on turvallistamisen teorian perusolettamuksia, vaikkakin muun muassa Vuori on argumentoinut vakuuttavasti sen puolesta, että turvallistamisen teoriaa voi soveltaa myös epädemokraattiseen päätöksentekoprosessiin. Turvallisuuspuhetta ja puhetekoja on mahdollista analysoida riippumatta kontekstista.[191]

Avainsana tässä tapauksessa on legitimiteetti. Wæverin ja Buzanin mukaan turvallistaminen on *erityispolitiikkaa* tai turvallisuusasioiden viemistä tavanomaisten poliittisten keinojen ulkopuolelle. Tätä voidaan kuvata sääntöjen rikkomisena. Perinteisemmän näkökulman mukaan, kun turvallisuuden logiikkaa ja retoriikkaa käytetään vakiintuneiden konventioiden rikkomiseen, puhutaan turvallistamisesta.[192] Vuoren näkökulman mukaan kaikilla kansallisvaltioilla on pyrkimys perusarvojensa turvaamiseen ja turvallistamisen teoria pyrkii tunnistamaan ja määrittämään näitä arvoja uhkaavat tekijät. Sääntöjen rikkominen tai eksistentiaalisen uhan tunnistaminen ei kuitenkaan itsessään vielä riitä turvallistamisen perusteiksi.[193] Legitimiteetti syntyy ainoastaan yleisön kautta.

### 4.2.4. Julkinen keskustelu kiihtyy

Helmikuussa 2017 julkaistiin raportti *”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi”,* joka otti voimakkaasti kantaa keskeneräiseen tiedustelulainsäädännön uudistukseen.

*Strategisen johtajuuden selkeyttäminen ja vahvistaminen ovat keskeinen asia Suomen kyberturvallisuuden vision saavuttamisen varmistamisessa. Tarvitaan*

[190] Buzan et al. artikkelissa Vuori 2008, 68.
[191] Vuori 2008, 66-67.
[192] ma. 2008, 69.
[193] Vuori 2008, 69-70.

*kybertoimintaympäristöön soveltuvan toimivaltuuksien ja johtamismallin luomista erityisesti laajamittaisten häiriötilanteiden hallinnassa. Johtaminen edellyttää kansallisen tason tilanneymmärryksen parantamista ja havaintokyvyn kehittämistä. Tässä suhteessa kansallisen tiedustelulainsäädännön aikaansaaminen on välttämätöntä.*[194]

Raportti kyseenalaistaa Suomen kyvyn suojautua kyberuhkia vastaan, samoin kuin poliittisen johdon sitoutumisen kyberturvallisuuden kehittämiseen. Raportti toteaa Suomen epäonnistuneen tavoitteessaan nousta vuoteen 2016 mennessä kyberturvallisuuden kärkimaaksi. Raportti vertaileekin Suomen kyberturvallisuusstrategiaa kuuden muun valtion[195] kanssa ja nostaa esiin sen, että kaikissa verrokkimaissa on käynnissä kyberturvallisuuslainsäädännön uudistus. Raportti argumentoi siis vahvasti sen puolesta, että nopeasti kehittyvällä alalla säädöspohja ei ole pysynyt muutoksen mukana tai on vanhentunutta, eikä siten enää palvele kyberturvallisuuden nykytarpeita.[196]

Raportin julkistamisen jälkeen useat poliitikot mukaan lukien Suomen pääministeri Juha Sipilä, silloinen sisäministeri Paula Risikko ja puolustusministeri Jussi Niinistö esittivät toivomuksensa siitä, että käynnissä oleva tiedustelulainsäädäntö vietäisiin kiireellisenä läpi eduskunnassa.[197]

Normaalissa perustuslain säätämisjärjestyksessä on linjattu, että eduskunnan hyväksyttyä lakiesityksen jätetään se lepäämään ja odottamaan seuraavaa, vaaleilla valittua eduskuntaa, jonka tulee vielä hyväksyä laki kahden kolmasosan enemmistöllä. Kiirehtimismenettely tarkoittaa, että nykyisen eduskunnan pitäisi antaa lakialoitteelle 5/6 hyväksyntä, jonka jälkeen muutokset lakiin pitää hyväksyä vielä samassa eduskunnassa kahden kolmasosan enemmistöllä. [198]

*- Tällä hetkellä Suomessa on mahdollisuus tiedustella ja saada tietoa, jos on kysymys rikoksesta tai sen suunnittelusta, mutta nyt meidän pitää saada paljon aikaisemmin tietoa, esimerkiksi jos jostain on uhkaa kansakunnalle, Risikko perusteli kiireellistä tarvetta.*[199]

*- Siinä on tehty erittäin hyvää työtä nyt parlamentaarisessa ryhmässä. Oma toivomukseni on se, että asia menisi kiireellisessä järjestyksessä [läpi eduskunnassa]. Sehän vaatii perustuslakimuutoksen. Se on selvä asia jo nyt. Parlamentaarinen ryhmä tekee töitä tämän kuukauden loppuun asti, Sipilä vastaa Lännen Median kysymykseen.*[200]

[194] Valtioneuvosto 17.2.2017
[195] Vertailukohteena olevat valtiot Alankomaat, Iso-Britannia, Israel, Ruotsi, Singpore ja Viro
[196] Raportti Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi, 2018, 62.
[197] Verkkouutiset 25.5.2017.
[198] Verkkouutiset 25.5.2017.
[199] Kaleva 1.3.2017.
[200] Kaleva 9.4.2017.

- *Toivottavasti muutos hyväksytään nopeutetusti, Sipilä painottaa LM:lle.*[201]

Keväällä 2017 uutisoitiin laajasti myös tasavallan presidentin Sauli Niinistön ottaneen kantaa tulevaan tiedustelulainsäädäntöön.

*”Hallitus ajaa tiedustelulainsäädännön uudistamista mahdollisimman nopeassa aikataulussa. Presidentti Sauli Niinistö tukee asian kiireellistä käsittelyä eduskunnassa.*

*– Olen nyt kolmen hallituksen aikana keskustellut kaikkien eduskuntapuolueiden puheenjohtajien kanssa tiedustelulainsäädännön saattamisesta ajan tasalle. Kun aloituksesta alkaa olla jo nelisen vuotta niin suhtaudun automaattisesti tähän niin, että niin pian kuin mahdollista.”*[202]

Loppukeväästä 2017 oikeusministeri Antti Häkkänen otti myös kantaa kiirehtimismenettelyyn mutta selvästi kriittisemmin äänenpainoin.

*”Oikeusministeri Häkkäsen mielestä perustuslain muuttamista kiirehtimismenettelyllä tulisi käyttää ”vasta aivan ääritapauksissa, poikkeuksellisissa tilanteissa”.*

*– Minusta meidän Suomessa kannattaa pitää todella pyhänä tätä perustuslain rajoittavaa roolia. Sen (kiirehtimismenettelyn) käyttöön pitää olla todella korkea kynnys, ministeri linjaa.”*[203]

Asiaa edistettiin asiantuntijatyön ja parlamentaarisin valmisteluin ennen esityksen antamista eduskunnalle. Uusi lakiehdotus esiteltiin huhtikuussa 2017 sisäministerille, puolustusministerille ja oikeusministerille ja lähetettiin sen jälkeen laajalle lausuntokierrokselle. [204] Kesään 2017 mennessä lausuntoja ja kommentteja saatiin yhteensä 64 kappaletta viranomaistahoilta, kansalaisjärjestöiltä ja liike-elämän edustajilta, joiden pohjalta joitakin lakipykäliä arvioitiin uudelleen ja tarkennettiin. [205]

Turvallistamisen teoria korostaakin turvallistamisen prosessissa valtuuttavan tai mahdollistavan yleisön olemassaoloa. Kaikki turvallistamisen teoreetikot lähtevät siitä oletuksesta, että turvallistamisyritys voidaan katsoa onnistuneeksi vain jos ehto tämän yleisön olemassaololle täyttyy ja tämä yleisö hyväksyy turvallistamisen kohteena olevat toimenpiteet. [206] Vuoren viitekehykseen peilaten tässä tulevien toimenpiteiden legitimoinnin voidaan katsoa

[201] Kaleva 9.4.2017.
[202] Sauli Niinistö Ylen uutisessa 21.4.2017.
[203] Antti Häkkänen Nykypäivä 25.5.2017.
[204] Yle uutinen 8.12.2017.
[205] Sisäministeriön tiedote 11.7.2017.
[206] Balzacq 2011, 35.

syntyvän lakia valmistelevan hallituksen ja kansalaisia edustavien kansanedustajien dialogissa.[207]

Tiedustelulaista mediassa käyty julkinen keskustelu oli vilkasta. Vastakkainasettelua ei nähty niinkään yksilönsuojan ja kansallisen turvallisuuden välillä vaan keskustelua on käyty nimenomaan perustuslakiin tehtävistä muutoksista ja muutoksen läpiviennin aikataulusta.

*”Pitäisi perustella, miksi on niin kiire, että meidän on sivuutettava demokraattinen kansalaiskeskustelu. Toistaiseksi en ole nähnyt perusteluja kiireellisyyden edellytyksistä.”*[208]

*”Tässä on – valtiosääntöoikeudellisesti – ongelmana se, että perustuslain muutosta viedään tiedustelulainsäädännön ehdoilla. Vaikka perustuslaki on perusta, johon sopeutetaan muu lainsäädäntö.”*[209]

Asiantuntijat ovat lähtökohtaisesti kritisoineet eniten puutteellista aikaa kansalaiskeskustelulle, sekä sitä miten muutoksen läpiviemistä 5/6 enemmistöllä perustellaan. Perustuslain läpivieminen nopeutettuna olisi ennakkotapaus, mikä näyttää myös linjaa tulevaisuudelle. [210]

Tämän tapaustutkimuksen ja turvallistamisen prosessin näkökulmasta on merkittävää, että poikkeuksellisesta lakiesityksestä pyritään käymään mahdollisimman laajaa julkista keskustelua. Siten turvallistamisen näkökulmasta kriteeri sille, että yleisöllä on *mahdollisuus kieltäytyä* täyttyy Vuoren esittämän viitekehyksen tapaan.[211]

### 4.2.5. Muuttunut toimintaympäristö, kiireellisyys korostuu

Yhtenä selkeimmin aineistosta esiin nousevana diskurssina korostuu kiireellisyys ja muuttunut toimintaympäristö. Asetelmassa turvallisuuspuhetta tuottavat ministerit ja viranomaistahot korostavat jokainen turvallisuusympäristön nopeaa muutosta.

*Suomen turvallisuusympäristö muuttuu nopeasti. Uudet uhat edellyttävät uudenlaista valmiutta ja varautumista.*[212]

*Globalisaatiosta ja digitalisoitumisesta johtuen, Suomen turvallisuusympäristö on muuttunut nopeasti. Turvallisuus- ja toimintaympäristön muutosten myötä kansallisen turvallisuuden uhat, kuten vakoiluun ja terrorismiin liittyvät ilmiöt ja hankkeet, tapahtuvat yhä useammin*

[207] Vuori 2008, 80.
[208] Tutkija Niklas Vainio, Yle uutinen 31.7.2017.
[209] Professori Veli-Pekka Viljanen, Yle uutinen 31.7.2017.
[210] Yle uutinen 31.7.2017.
[211] Vuori 2008, 80.
[212] Sisäministeriön tiedote 19.4.2017.

*tietoverkoissa. Tämä muutos edellyttää myös kybertoimintaympäristöön ulottuvia viranomaisvaltuuksia. Uuden tilanteen myötä on Suomessakin aloitettu sisäministeriön ja puolustusministeriön toimialoilla tiedustelulainsäädännön valmistelut.*[213]

*Turvallisuustilanteen kiristymisellä Euroopassa ja Itämeren alueella on vaikutuksia Suomelle. Kansainvälisen tilanteen kiristymisestä huolimatta Suomeen ei kohdistu välitöntä sotilaallista uhkaa. Sotilaalliseen voimankäyttöön Suomea vastaan tai sillä uhkaamiseen on kuitenkin varauduttava.*[214]

Tulevaisuuden toimenpiteitä *perustellaan* muuttuneella tilanteella. Turvallisuuspuheen painopiste suuntautuu yhä enemmän viranomaisten keskinäisestä keskustelusta kohti laajempaa julkista keskustelua. Keskustelun laajetessa ja kesän 2017 myötä diskurssit muuttuvat selkeämmin uhkan sävyttämiksi, mistä olen nostanut seuraavaan lukuun joitakin esimerkkejä.

### 4.2.6. Uhkan diskurssi voimistuu

Tämän tapaustutkimuksen näkökulmasta kesä 2017 oli merkityksellinen kahdella tapaa. Kesäkuussa 2017 suojelupoliisi päivitti uhka-arviotaan ja raportoi nostaneensa Suomen tasolle kaksi (neliportaisella asteikolla), mikä määrittelee uhkan *kohonneeksi*. Kohonnutta uhka-arviota perusteltiin kasvaneella suojelupoliisin tietoon tulleilla terrorismiin liittyvien hankkeiden ja suunnitelmien määrällä ja yleisellä *terrorismitrendin* kasvulla.[215]

18.8.2017 eli vain kaksi kuukautta myöhemmin Suomessa uutisoitiin ensimmäisestä epäillystä terroriteosta. Turussa puukotettiin kymmentä ihmistä, joista kaksi kuoli. Tämän seurauksena suojelupoliisi käynnisti tutkimukset puukotuksista terroristisena tarkoituksena tehtyinä murhina ja murhan yrityksinä. [216] Vain kaksi päivää tapahtuneen jälkeen muun muassa presidentti Sauli Niinistö kommentoi Turun iskua medialle:

*”Niinistöltä kysyttiin muun muassa, miten mahdollisia uusia iskuja voitaisiin estää. Pian vastaus kääntyi tiedustelulainsäädäntöön. Presidentti sanoi toivovansa tiedustelulainsäädännön tulevan voimaan.*
*– Näissä asioissa täytyy nyt kyllä toimia pikaisesti.*
*Myöhemmin hän lisäsi, että uskoo Turun tapahtumien jouduttavan tiedustelulain käsittelyä.”*

[213] Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017 – 2020, 2017, 5.
[214] Valtioneuvoston puolustusselonteko 2017, 14.
[215] Yle uutinen 14.6.2017.
[216] Yle uutinen 19.8.2017.

Turvallistamispyrkimyksen ja tulevaisuuden toimenpiteiden legitimoinnin näkökulmasta ei ole merkityksetöntä, että presidentti esittää julkisia lausumia ja toiveensa tiedustelulainsäädännön nopeasta käsittelystä. Esimerkiksi Thierry Balzacqin mukaan turvallistaminen voi olla diskursiivista tai ei-diskursiivista, tahallista tai tahatonta, performatiivista tai toimintaan ohjaavaa olematta kuitenkaan itsessään toimintaa. Siten turvallisuusongelmat voivat syntyä tietoisen toiminnan tuloksena tai nousta esiin sellaisista käytännöistä, joiden tarkoituksena ei alun perin ole ollut luoda uusia turvallisuusongelmia.[217] Siten tulkittuna sekä Turun tapahtumat, että presidentin aktiivinen osallistuminen tiedustelulakikeskusteluun on omalta osaltaan voinut vaikuttaa turvallistamisprosessiin joko tietoisen tai tiedostamattoman toiminnan seurauksena.

Alkusyksystä 2017 julkaistiin lausuntokierroksen tulokset. Lausuntokierros kirvoitti paljon kannanottoja niin viranomaistahoilta kuin elinkeinoelämän edustajilta. Sisäministeriön arvioiden mukaan lain uudistamista ja kansallista turvallisuutta pidetään sekä tarpeellisena, että hyvänä tavoitteena ja lausuntoja ylipäätään pääsääntöisesti myönteisinä, vähemmistön suhtautuessa ehdotukseen kriittisesti.[218] [219]

Suurin kritiikkiä ja keskustelua herättänyt asia liittyy kansallisen turvallisuuden diskurssiin. Esitystä on kritisoitu siitä, että kansallisen turvallisuuden käsitettä on vaikea tyhjentävästi määrittää ja että on riskinä, että kansallisen turvallisuuden käsite lähenee liiaksi yleisen turvallisuuden käsitettä.[220] Tiedustelulainsäädäntöä kritisoineet tahot ovat kannanotoissaan viljelleet diskursseja *massavalvonnasta verkkourkintaan* pyrkien näin vahvistamaan mielikuvaa tiedustelulaista yksityisyyden suojaa rajoittavana tai sitä jopa loukkaavana lakina.[221] Terrorismia ei pidetä eksistentiaalisena uhkana, jonka vuoksi olisi perusteltua tehdä muutoksia perustuslakiin, varsinkaan nopeutetussa aikataulussa. [222]

Joulukuussa 2017 nähtiin tiedustelulainsäädäntövalmistelun ehkä poikkeuksellisin episodi. Helsingin Sanomien haltuun oli päätynyt salassa pidettäväksi luokiteltua materiaalia, jossa

[217] Balzacq 2011, 2.
[218] Sisäministeriön tiedote 7.9.2017.
[219] Lausuntoyhteenveto 2017, 15.
[220] Effin lausunto Yle uutinen 21.1.2017.
[221] Yle uutinen 21.1.2017.
[222] IKI:n lausunto Yle uutinen 21.1.2017.

käsiteltiin tiedustelulain valmistelua puolustusvoimien osalta. Uutisessa luonnehdittiin tiedustelulainsäädäntöä mullistavaksi:

*”Sana mullistaa ei ole liioiteltu, sillä sotilastiedustelun tehtävistä tai toimivaltuuksista ei ole Suomessa omaa kattavaa lainsäädäntöä. Siksi sotilastiedustelu on kehittänyt itselleen salaisia toimintamalleja, joita ei ole koskaan hyväksytty eduskunnassa eikä avattu ulkopuolisille.”*[223]

Tämä avaa mielenkiintoisen näkökulman myös tämän tutkimuksen näkökulmasta. Peilaten turvallistamistyypeistä ainoaan, joka turvallistaa jo toteutettuja poikkeuksellisia toimenpiteitä eli *aiempien toimenpiteiden legitimointiin,* voidaan olettaa että mahdollisesti tulevaisuudessa hyväksyttävä tiedustelulaki toteutuessaan mahdollistaa kyseisen turvallistamistyypin todentamisen.

Helsingin Sanomat sai käsiinsä kiistellyn lakiesityksen keskeiset kohdat jo ennen asian virallistamista. Joulukuun alussa julkaistun uutisen mukaan suurimmat muutokset uudistetussa tiedustelulaissa koskevat suojelupoliisin roolia ja valtuuksia tiedustelutoimintaan liittyen. Uudistetun tiedustelulain mukaan suojelupoliisi voisi hankkia tiedustelumenetelmillä tietoa seuraavista kansallista turvallisuutta vakavasti uhkaavista toiminnoista.[224]

*1) terrorismista;*
*2) ulkomaisesta tiedustelutoiminnasta;*
*3) joukkotuhoaseiden suunnittelusta, valmistamisesta, levittämisestä ja käytöstä;*
*4) kaksikäyttötuotteiden vientivalvonnasta annetun lain (562/1992) 2 §:ssä tarkoitettujen kaksikäyttötuotteiden suunnittelusta, valmistamisesta, levittämisestä ja käytöstä;*
*5) kansanvaltaista yhteiskuntajärjestystä uhkaavasta toiminnasta;*
*6) suuren ihmismäärän henkeä tai terveyttä taikka yhteiskunnan elintärkeitä toimintoja uhkaavasta toiminnasta;*
*7) vieraan valtion toiminnasta, joka voi aiheuttaa vahinkoa Suomen kansainvälisille suhteille, taloudellisille tai muille tärkeille eduille;*
*8) kansainvälistä rauhaa ja turvallisuutta uhkaavasta kriisistä;*
*9) kansainvälisten kriisinhallintaoperaatioiden turvallisuutta uhkaavasta toiminnasta;*
*10) Suomen kansainvälisen avun antamisen ja muun kansainvälisen toiminnan turvallisuutta uhkaavasta toiminnasta; sekä*
*11) yhteiskuntajärjestystä uhkaavasta kansainvälisestä järjestäytyneestä rikollisuudesta.*

Merkittävin kaavailtu muutos siviilitiedustelulainsäädäntöön liittyy suojelupoliisin roolin ja tiedusteluvaltuuksien laajentamiseen. Käytännössä uudistus tarkoittaisi supon muuttumista poliisiorganisaatiosta tiedusteluorganisaatioksi.[225] Samoin puolustusvoimat saisivat laajat tiedusteluvaltuudet. Esityksen mukaan tarvittavan tiedonhankinnan kohteena olevan toiminnan

[223] Helsingin Sanomat 16.12.2017.
[224] Yle uutinen 8.12.2017.
[225] Yle uutinen 21.4.2017.

ei välttämättä tarvitsisi olla rangaistavaksi säädettyä tai edes edennyt niin pitkälle, että sitä voitaisiin konkreettisesti pitää rikollisena toimintana.[226]

Esitys luottamuksellisen viestin suojaa koskevan perustuslain säännöksen muuttamisesta eduskunnalle annettiin viimein 25.1.2018.

*Tiedustelumenetelmien tarkoituksena olisi tuottaa välttämätöntä tietoa kansallista turvallisuutta vakavasti uhkaavasta toiminnasta ylimmän valtiojohdon päätöksenteon tueksi sekä kansallisen turvallisuuden suojaamiseksi. Suomen turvallisuusympäristö muuttuu nopeasti, ja uudet uhat edellyttävät uudenlaista valmiutta ja varautumista.[227]*

*Tietoa sotilaallisesta toiminnasta ja sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta, on esityksen mukaan välttämätöntä hankkia myös sellaisilla tavoilla, jotka saattavat rajoittaa luottamuksellisen viestin salaisuuden suojaa nykyaikaisessa viestinnässä. [228]*

Samalla hallitus ehdotti, että eduskunta käsittelisi perustuslain muutosesityksen kiireellisessä perustuslainsäätämisjärjestyksessä.

*Hallitus ehdottaa, että eduskunta käsittelisi perustuslain muutosesityksen kiireellisessä perustuslainsäätämisjärjestyksessä. Suomen turvallisuustilanteen heikentyminen ja tarve varautua Suomen kansallista turvallisuutta uhkaavaan toimintaan muodostavat hallituksen näkemyksen mukaan sellaisen poikkeuksellisen tilanteen, jossa perustuslain kiireelliselle muuttamiselle on osoitettavissa välttämätön tarve.[229]*

Turvallistamispyrkimykset ovat tulleet aiempaa ilmeisemmiksi retoriikan ja diskurssien voimistuessa selvästi lakiehdotuksen tultua viralliseen käsittelyyn.

*”Hybridivaikuttaminen on jo arkipäivää poliittisten tavoitteiden saavuttamiseksi tai vastustajien häiritsemiseksi”, perusteli sisäministeri Kai Mykkänen (kok) puheenvuorossaan.*

*Vasta helmikuun alussa sisäministeriksi siirtynyt Kai Mykkänen (kok) sanoi tiistaina, että jokainen kriittisiin tietojärjestelmiimme asennettu ”kyberpommi” on liikaa, jos se olisi voitu lainsäädännöllä estää.*

[226] Oikeusministeriön tiedote 25.1.2018.
[227] Sisäministeriön tiedote 25.1.2018.
[228] Sisäministeriön tiedote 25.1.2018.
Sanamuodon ja sen nykyisen tulkintakäytännön mukaan ”..lailla ei voida säätää viestin suojan rajoittamisesta muissa tarkoituksissa, kuten esimerkiksi kansallisen turvallisuuden suojaamiseksi..” ja siihen kohdistuviin uhkiin varautumiseksi. Tämän mahdollistamiseksi perustuslakiin lisättäisiin uusia hyväksyttäviä perusteita rajoittaa luottamuksellisen viestin salaisuutta. Esityksen mukaan viestin suojaa voitaisiin rajoittaa, jos se olisi välttämätöntä ”tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.
[229] Oikeusministeriön tiedote 25.1.2018.

Kyberpommeihin viittaamista voidaan pitää kohtalaisen latautuneena retoriikkana, mikä yhdistettynä näiden uhkien arkipäiväistymiseen tekee puheaktista tavoitteeltaan vaativan, siihen yhdistyy sekä ’asia on näin’ toteamista, että varoitus, mikä on tulkittavissa lausunnon takaa.

Normaalia perustuslainsäätämisjärjestystä noudattaen, tiedusteluviranomaisten toimivaltuuksia koskevat säännökset voisivat tulla aikaisintaan voimaan vuoden 2020 alussa. Käytettäessä kiireellistä perustuslainsäätämisjärjestystä muutokset olisi mahdollista saada voimaan jo vuoden 2018 loppupuolella.[230]

### 4.2.7. Kohti loppunäytöstä - ja turvallistettua lopputulosta

Syyskuun alussa 2018 eduskunnan perustuslakivaliokunta otti hallituksen esityksen tiedustelulakipaketista käsittelyyn[231] ja hyväksyi sen tietyin huomautuksin ja muutosehdotuksin. [232] [233] Perustuslakivaliokunta esitti myös uuden lain voimaantulopäiväksi helmikuun 1. päivää 2019.

Eduskunta äänesti perustuslain muutoksesta kiireellisenä 2.10.2018. Muutosehdotus hyväksyttiin eduskunnassa äänin 178 - 13, mikä mahdollistaa tiedustelulakien läpiviemisen vielä tällä vaalikaudella.[234] Suomen tasavallan presidentti Sauli Niinistö vahvisti perustuslain muutoksen 4.10.2018.

*Perustuslakia ei ole aiemmin muutettu kiireellisesti uuden perustuslain aikana eli vuoden 2000 jälkeen. Itse perustuslain muutoksen osalta eduskunta siis käytti nopeutettua lainsäätämisjärjestystä ensimmäistä kertaa.[235]*

Tätä tutkimusta kirjoittaessa, esitykset ovat edelleen eduskunnan valiokuntien käsittelyssä.

[230] Oikeusministeriön tiedote 25.1.2018.
[231] Helsingin Sanomat 5.9.2018.
[232] Eduskunnan perustuslakivaliokunnan mietintö PeVM 9/2018 vp.
[233] Helsingin Sanomat 21.9.2018.
[234] Helsingin Sanomat 3.10.2018.
[235] Helsingin Sanomat 5.10.2018.

## 4.3. Uhkan diskurssi muutoksessa

Kyberturvallisuus representoituu[236] ensisijaisesti sitä uhkaavien tekijöiden ja toimijoiden kautta. Erityisinä uhkina toistuvasti esiin nostetaan esimerkiksi terrorismi, vieraiden valtioiden Suomeen kohdistama vakoilu tai elintärkeän infrastruktuurin lamauttaminen.[237] Uhkadiskurssin rakentamisessa korostuvat erityisesti uudenlaiset, ei valtiolliset toimijat ja perinteisen valta-asetelman muuttuminen. Ensimmäisiä kertoja tunnustetaan se, että kybermaailmassa ei päde perinteinen valtioiden välinen voimapolitiikka vaan ”Se [kybertoimintaympäristö] antaa pienillekin valtioille ja ei-valtiollisille toimijoille mahdollisuuden toimia tehokkaasti. Kybermaailmassa suuruus ja massa eivät enää ole hallitsevia, vaan osaaminen”.[238]

Kyberoperaatioihin viitatataan ja niitä tulkitaan niin kutsutuiksi pehmeiksi toimiksi, mikä asiantuntijoiden mielestä alentaa niiden käyttökynnystä.[239] Toisaalta tehdään vertailua muihin valtioihin ja erityisesti suurvaltoihin, missä ”Suurvallat ovat rinnastaneet kyberhyökkäykset sotilaallisiin toimiin, joihin voidaan vastata kaikin mahdollisin keinoin.”[240]

Viranomaistahoista puolustusministeriö, sisäministeriö ja oikeusministeriö rakentavat omien tiedotteidensa ja uutistensa kautta voimakkaasti uhkan diskurssia. Merkittävää tutkimuksen kannalta on kiinnittää huomiota aineistosta esiin nousevaan uhkan diskurssin voimistumiseen vertaamalla tutkimusaineiston alkupään tekstejä (vuodesta 2013) vuoden 2018 teksteihin. Saman havainnon voi tehdä tiedustelulainsäädännön uudistamiseen liittyvistä tiedotteista vuosien 2015 ja 2018 välillä. Erityisesti vuoden 2017 Suomen kyberturvallisuuden tilaa selvittävän raportin jälkeen viranomaistahojen kannanotot ovat tiukentuneet, tarkentuneet ja muuttuneet selkeästi uhkaa korostaviksi ja tiedustelulainsäädännön muutosta puoltaviksi.

*Kybertoimintaympäristöön kohdistuvat uhkat ovat muuttuneet vaikutuksiltaan aiempaa vaarallisemmiksi yksittäisten ihmisten, yritysten sekä koko yhteiskunnan kannalta. Uhkia muodostavat toimijat ovat ammattimaisempia kuin ennen ja nykyään niihin voidaan laskea kuuluviksi myös valtiolliset toimijat. Kybertoimintaympäristössä toteutettavia hyökkäyksiä voidaan käyttää poliittisen ja taloudellisen painostuksen välineinä ja vakavassa kriisissä yhtenä vaikuttamiskeinona perinteisten sotilaallisten voimakeinojen ohella.*[241]

Uhkan diskurssi on kuvailevaa ja tuntemattoman uhan mielikuvaa vahvistavaa. Tuntemattomuus ja epävarmuustekijät korostuvat, vihollisella ei ole nimeä tai kasvoja, mikä

[236] Pietikäinen et al. 2009, 41-42
[237] Sisäministeriön tiedote 19.4.2017
[238] Suomen kyberturvallisuusstrategia 2013, 17.
[239] Suomen kyberturvallisuusstrategia 2013, 17.
[240] Suomen kyberturvallisuusstrategia 2013, 17.
[241] Suomen kyberturvallisuusstrategia 2013, 1.

lisää uhan pelottavuutta. Tämä näkyy analysoitavissa teksteissä ja otteissa sen korostamisena, että sekä uhkan muodostavat toimijat, että uhkaavat toimet ovat uusia.

Tässä turvallistamistyypissä korostuu myös diskurssijärjestys. Auktoriteetin asema korostuu, kun ministerit tai tasavallan presidentti ottaa kantaa tiedustelulakiin, on sillä huomattavasti suurempi painoarvo kuin sillä jos asiantuntijataho esittää samanlaisen kannan. Perustamme luottamuksemme kokemukseen ja representaation kautta, tietyillä instituutioilla on suurempi äänenpaino. [242]

Turvallistamisen teorian näkökulmasta myös deterrenssi eli pelote on läsnä vaikkei välittömästi näkyvillä. Osaltaan voidaan argumentoida, että Suomen viranomaistahojen puheteot ja diskurssit pyrkivät omalta osaltaan luomaan deterrenssiä. On perusteltua olettaa, että koveneva tiedustelulainsäädäntö ja siten kiinnijäämisen mahdollisuus toimivat myös pelotteena kyberrikollisuusryhmiä vastaan. Samoin uhkan ja siten mahdollisten toimenpiteiden kohteiden nimeäminen alleviivaa samaa; sisäministeriön verkkosivuilla[243] ja useissa tiedotteissa viitataan suoraan rikollisiin, terroristeihin tai ulkomaisiin vakoojiin.[244]

*Suomen sotilas- ja siviilitiedustelulla olisi jatkossa huomattavasti suuremmat valtuudet tiedustella – omia tarpeitaan varten sekä vaihtotavaraksi muiden tiedustelupalvelujen kanssa.*[245]

## 4.4. Turvallistamisen mekanismit käytössä

Analyysiosio on pyrkinyt tuomaan esiin niitä mekanismeja ja erityisesti puhetekoja, millä kyberturvallisuutta on turvallistettu Suomessa viimeisten viiden vuoden aikana. Aineistosta voi selkeästi tunnistaa turvallistamisen tyypeistä sekä *agendalle nostamisen*, että *tulevien toimenpiteiden legitimoinnin*. Myös *deterrenssin* käytöstä ja mahdollisuudesta *aiempien toimenpiteiden legitimointiin* nousee paikoitellen esiin viitteitä.

Aineiston ja analyysiosion valossa näyttää siltä, että kyberturvallisuuteen liitettävä turvallistamisen prosessi on edennyt vuodesta 2013 lähtien kohti turvallistettua lopputulosta.

[242] Pietikäinen et al. 2009, 46.
[243] Sisäministeriön verkkosivut ”Tiedustelulain tarpeeseen liittyviä käytännön esimerkkejä”.
[244] Sisäministeriön tiedote 25.1.2018.
[245] Helsingin Sanomat 19.12.2017.

Turvallistamisen prosessin näkökulmasta jo perustuslakiin tehtävät muutokset voidaan katsoa poikkeukselliseksi, mutta viimeistään näiden muutosten kiirehtiminen ja nopeutettuun lainsäädäntöjärjestykseen turvautuminen täyttää näkökulmastani turvallistamisen kriteerit.

Seuraavassa, johtopäätöksiä käsittelevässä luvussa, tarkastelen tarkemmin tutkimuksen tuloksia suhteutettuna tutkimuskysymyksiin ja pohdin laajemmin tutkimuksen merkitystä.

# 5. JOHTOPÄÄTÖKSET

Kybertoimintaympäristön tuleminen osaksi turvallisuusympäristöämme näyttäytyy monin tavoin. Tietoyhteiskuntana olemme riippuvaisia tietoverkoista ja niihin liittyvien järjestelmien toiminnasta ja siten myös alttiita niihin kohdistuville häiriöille tai uhille. [246] Vuoden 2013 kyberturvallisuusstrategiasta on viiden vuoden aikana siirrytty toimenpide-esityksistä kohti konkretiaa. Samaa tahtia kasvaneiden tietoturvauhkien ja ymmärryksemme kasvun myötä myös kyberturvallisuuteen kohdistuva retoriikka on koventunut. Vihollinen on edelleen kasvoton mutta sitäkin vaarallisempi, uhan koetaan uhkaavan kansallista turvallisuutta ja siten koko olemassaolomme edellytyksiä.

Tämän tutkimuksen alussa asetin tavoitteeksi ymmärtää paremmin suomalaista kyberturvallisuusajattelua, tarkastellen sitä, miten kyberturvallisuutta pyritään turvallistamaan poliittisessa diskurssissa, luonnollisesti peilaten sitä samalla laajempaan teoreettiseen viitekehykseen ja kyberturvallisuuden tutkimukseen. Erityisesti halusin etsiä vastauksia kysymyksiin siitä, millä tavalla kyberturvallisuudesta ja tiedustelulaieista puhutaan julkisuudessa ja sen millaisia päätelmiä empiirisen tapaustutkimuksen avulla ja tiedustelulaki -esimerkkiä käyttäen voimme tehdä Suomen kyberturvallisuuskeskusteluun liitetystä turvallistamisprosessista.

Tapauksena tiedustelulaki on yksi aikamme hengen representaatio, muutaman vuoden päästä tuskin enää muistamme koko keskustelua mitä on kiivaasti käyty viimeiset vuodet. Tapaustutkimus todentaa kuitenkin erinomaisesti sen, millaisia turvallistamisen prosesseja tässä kontekstissa on sekä samanaikaisesti, että ajallisena jatkumona havaittavissa. Esimerkkiaineisto, joka tässä rajattiin tiedustelulakia koskeviin tiedotteisiin ja uutisiin vuosina 2015-2018 on nostanut hyvin esiin useita turvallistamisen tyyppejä, joista vahvimmin esiintyvät agendalle nousu ja tulevien toimenpiteiden legitimoinnin -tyypit.

Agendalle nousu tapahtui vuonna 2015. Legitimointi käynnistyi samassa aikaikkunassa mutta koki selkeän momentumin kasvun vuoden 2017 kesästä vuoden 2018 syksyyn. Nämä kaksi

[246] Suomen kyberturvallisuusstrategia 2013, 1.

turvallistamisen tyyppiä nousevat selkeimmin aineistosta esiin ja osoittavat erityisesti perustuslainsäädännön kiirehtimisvaatimuksen myötä sekä agendalle nostamisen, että legitimiteettimekanismien käyttöä. Aineistosta on poimittavissa myös viitteitä kolmannesta turvallistamisen tyypistä eli deterrenssivaikutuksesta mutta ei läheskään samassa mittakaavassa kuin kahden ensimmäisen tyypin kohdalla. Tämä heijastelee osin demokraattisen valtion ja parlamentaarisen järjestelmän olemassaoloa, turvallistaminen tapahtuu ensisijaisesti vetoamalla yleisöön ja argumentoimalla esityksen puolesta, sen sijaan että maalailtaisiin uhkakuvia.[247] Aineisto raottaa myös mahdollisuutta tulevaisuudessa menneisyyden toimenpiteiden legitimointi -turvallistamistyypin käyttöön viittaamalla puolustusvoimien toimintamalleihin ja -tapoihin, jotka eivät mahdollisesti kestä päivänvaloa nykyisen lainsäädännön valossa.[248]

Turvallistamisen tämän tapaustutkimuksen kontekstissa voidaan katsoa edenneen lineaarisesti yhdestä vaiheesta seuraavaan; Ensimmäinen turvallistaminen tapahtui jo siis vuosien 2013-2015 aikana kun kyberturvallisuus nostettiin onnistuneesti turvallisuusagendalle. Päätös tiedustelulainsäädännön uudistamisesta on tästä onnistunut osoitus. Sitä seurannut keskustelu perustuslakiin tehtävistä muutoksista käynnisti turvallistamisen seuraavan vaiheen, minkä loppusanat ovat tätä kirjoittaessa enää viimeistä silausta vaille.

Turvallistamisen prosessi nähdään tyypillisesti janana, jonka toisessa päässä on epäpoliittisena pidetyt asiat, keskivaiheilla selvästi politisoituneet julkisessa keskustelussa olevat asiat ja toisessa ääripäässä turvallistetut asiat, jotka ovat jo poliittisen keskustelun ulkopuolella, valmiiksi hyväksyttyjä ja välittömiä toimenpiteitä vaativia ongelmia.[249] Tämän tutkimuksen kontekstissa sijoitumme janalle suunnilleen sen keskivaiheille mutta suunta on kohti turvallistettua ääripäätä. Perustuslain muutoksen hyväksymistä ja kiireellisen lainsäädäntöjärjestyksen läpimenoa syksyllä 2018 voidaan pitää täydellisenä oppikirjaesimerkkinä onnistuneesta turvallistamisesta ja osoituksena siitä, että turvallisuuskysymys on siirtymässä poliittisen keskustelun ulkopuolelle. Siirrymme siis janalla kohti turvallistettua kybertoimintaympäristöä.

[247] Vuori 2008, 80-82.
[248] Helsingin Sanomat 16.12.2017.
[249] Korhonen teoksessa Politiikan Nykyteoreetikkoja 2008, 250.

Tämä on merkityksellistä siksi, että tutkimus osoittaa toteen sen, että myös Suomessa tapahtuu turvallistamista ja meidän tulisi olla perillä turvallistamisen mekanismeista ylintä poliittista johtoa myöten.

Tämä tutkimus ei ottanut kantaa tiedustelulainsäädännön sisältöön tai lainsäädännön tarpeellisuuteen, vaan sen pyrkimys oli tarkastella turvallistamisen prosessia kyberturvallisuuskeskustelun ja tiedustelulainsäädäntöuudistuksen kontekstissa. Tutkimuksen kohteena oli ensisijaisesti turvallisuuspuhe ja ne diskurssit, joilla joko turvallisuuden tai uhkan mielikuvia vahvistetaan, sekä turvallistamisen mekanismit, joita turvallisuuspuheen avulla vahvistetaan.

Turvallistaminen nähdään ensisijaisesti prosessina, mitä voidaan tarkastella seuraavien kysymysten avulla; kuka voi tehdä tai puhua turvallisuutta, mistä asioista, millä ehdoilla ja millä vaikutuksin?[250] Tapaus tiedustelulainsäädännön uudistus on osoittanut meille, että Suomessa kyberturvallisuuteen liittyvää keskustelua on hallinnut hallitus ja erityisesti puolustusministeri, sisäministeri ja oikeusministeri kannanottoineen. On kuitenkin merkittävää, että myös pääministeri ja tasavallan presidentti ovat julkisesti osallistuneet keskusteluun. Tässä tapauksessa he siis toimivat kaikki osaltaan turvallistamisen aktoreina.

Jokaisen empiirisen turvallistamisen tutkimuksen täytyy määrittää myös oma yleisönsä.[251] Tässä tutkimuksessa turvallistamisen kohdeyleisö on ollut primääristi koko Suomen kansa ja erityisesti eduskunta kansan edustajan roolissaan. Fokus on hieman vaihdellut turvallistamistyypin ja ajanjakson mukaan. Alkujaan lainsäädäntöuudistuksesta tiedotettaessa pääasiallinen yleisö muodostui virkamiehistä ja muista lainsäädäntöuudistukseen osallistuvista toimijoista. Lausuntokierroksella yleisö laajentui kattamaan monipuolisesti toimijoita eduskuntapuolueiden lisäksi kansalaisjärjestöistä yritysmaailman edustajiin. Siinä kohtaa julkinen keskustelu asiasta oli kohtuullisen vilkasta mutta värikkäimmät kannanotot ja selvästi aktiivisin vaihe julkisessa keskustelussa on käyty keväällä 2018 lakiesityksen antamisen jälkeen.

[250] Vultee teoksessa Balzacq 2011, 77.
[251] Vuori 2008, 72.

Tutkimuksellisesta näkökulmasta katsottuna valittu aihe soveltui erinomaisesti tutkimuksen tekemiseen. Se toimi erityisen hyvin myös ajankohtaisuutensa vuoksi. Lähestymistapana turvallistamisen teoria tarjosi oivan viitekehyksen, ja erityisen paljon koin että Juha A. Vuoren turvallistamistyyppien kategorisointi tuki tutkimuksen etenemistä ja toimi loogisena mallina aineistoa läpikäydessä.

Kaiken takana ovat kuitenkin puheaktit ja lopulta diskurssit niiden takana, konstruoimamme todellisuus sanojen ja käsitteiden takana. Merkittävää koko tutkimuksen ja varsinkin tulevaisuuden kannalta on se, että viiden vuoden takaiset kybertoimintaympäristöön liitetyt positiiviset diskurssit voimavarana ja mahdollisuutena loistavat nyt poissaolollaan. [252] Kyberturvallisuuteen liittyvä julkinen keskustelu on yhä enemmän uhkan diskurssia.

Laadullisen tutkimuksen tavoitteena on pyrkiä ymmärtämään tietystä ilmiöstä mahdollisimman paljon. Siitä näkökulmasta katsottuna voin yhtäaikaisesti olla sekä hyvilläni, että huolissaan. Toisaalta parlamentaarinen järjestelmämme näyttäytyy positiivisessa valossa sen mahdollistaessa avoimen, julkisen keskustelun ja lakimuutosten kritiikin. Olemme siis avoimia myös kyberturvallisuudesta käytävälle keskustelulle. Toisaalta olen huolissani siitä, että nojaamme kansalaisina omassa päätöksenteossamme voimakkaasti auktoriteetteihin. Kysymys kuuluu, hyväksymmekö asioiden turvallistamisen liian helposti? Perustuslain muutos, varsinkin kiirehdittynä herättää enemmän huolta kuin huojennusta. Tuleeko kiirehtimisjärjestyksestä uusi normaali? Olemmeko säätämässä perustuslakia riittävin perustein? Mitä kaikkea muuta tulevaisuudessa voidaan turvallistaa vetoamalla tuntemattomaan, bittiavaruudesta meihin kohdistuvaan uhkaan?

Turvallistamisen tutkimus alleviivaa turvallisuuspuheen tuottamisen merkitystä ja sitä tekevien toimijoiden ja puhetta tulkitsevien analyytikoiden vastuullisuutta asiassa, teemme joka päivä valintoja sen suhteen miten ja mihin viitekehykseen asetamme kulloisenkin turvallisuutta mahdollisesti uhkaavan asian.[253]

Tutkimusprosessi on osoittanut myös sen, että kokonaisuutena kyberturvallisuuden tutkimus on vielä lapsenkengissään. Tästä kertoo perinteisten teoreettisten koulukuntien haluttomuus

[252] Suomen kyberturvallisuusstrategia 2013, 1.
[253] Buzan et al. kirjassa Eriksson & Giacomello 2007, 60.

käsitellä kyberturvallisuutta omana tutkimusalueenaan. Kööpenhaminalainen koulukunta on viitoittanut tietä, jonka päälle nykyteoreetikot rakentavat omia mallejaan. Buzanilaisittain ajateltuna, pelkkä "turvallisuus" sana ei riitä luomaan mielikuvaa tietyn käsitteen tai konseptin vaikutuksesta yksilön turvallisuuteen. Turvallistamisen käsite vaatii aina mielikuvan myös erityisistä toimenpiteistä tai kiireellisyyden tunteesta ja määritellyn yleisön hyväksynnän saavuttaakseen yleisesti hyväksytyn leiman turvallisuusongelmana.[254]

Sama on siis kyberturvallisuuden kohtalo osana turvallisuudentutkimusta. Ennen kuin se hyväksytään täysimääräisesti muiden turvallisuussektorien joukkoon, tulee sen saavuttaa laajemman tutkimusyhteisön hyväksyntä. Kybertoimintaympäristön merkitys ylipäätään modernin yhteiskunnan ja olemassaolomme mahdollistajana asettaa sen ristiriitaiseen asemaan. Samoin kuin globaalit talouden rakenteet, on niiden järkkymisellä laajakantoisia seurauksia mutta toisaalta on olemassa vielä useita yhteiskuntia, jotka eivät ole samalla tavalla riippuvaisia informaatioverkoista. Välillisesti ja nimenomaan talouden mekanismien tullessa koko ajan riippuvaisemmaksi toimivasta kybertoimintaympäristöstä, olisi sen mahdollisilla häiriöillä seurauksia, jotka näkyisivät kaikkialla, riippumatta yksittäisen maan informaatioarkkitehtuurista.

Suomen kyberturvallisuusstrategiassa on paljon hyvää. Monella sektorilla toimenpideohjelman esittämät toimet ovat edenneet ja olemme kyenneet luomaan pohjaa tulevaisuudelle. Toisaalta allekirjoitan kyberturvallisuusselonteon tekijöiden huolen siitä, että emme riittävästi vielä ymmärrä muuttunutta toimintaympäristöä ja sen meille asettamia vaatimuksia.

Kybertoimintaympäristö ei tunnusta maarajoja ja on siten luonteeltaan aina globaalia toimintaa. Siitä syystä se muodostaa turvallisuudentutkimuksen osana tärkeän osan myös kansainvälisen politiikan tutkimusta.

Kyberturvallisuus ilmiönä on yhdelle tutkimukselle tarpeettoman laaja kokonaisuus, siitä syystä pyrin representoimaan kyberturvallisuudesta käytävää keskustelua ja siitä esiin kumpuavia turvallisuusdiskursseja turvallistamisen teoriaan peilaten case esimerkin kautta. Tähän tutkimukseen valitsin ajankohtaisen mutta tutkimusta hyvin tukevan case esimerkin; Suomen tiedustelulainsäädännön valmistelun vuosilta 2015-2018.

[254] Vultee teoksessa Balzacq 2011, 77.

Näen aiheessa myös mahdollisuuden jatkotutkimukseen; esimerkiksi muutama vuosi tiedustelulainsäädännön voimaanastumisen jälkeen olisi mielekästä päivittää tämäkin tutkimus vastaamaan muuttunutta todellisuutta – miten turvallistamisen prosessi on edennyt ja löydämmekö uusia viitteitä esimerkiksi muista turvallistamisen tyypeistä, kuten aiempien toimenpiteiden legitimoinnista ja deterrenssistä? Näihin keskittymällä voisi aikaansaada kokonaan oman tutkimuksen. Samoin tulevaisuudessa lain jo oltua muutamia vuosia voimassa, voisi turvallistamisen näkökulmasta saada riittävästi aineistoa irti myös kontrolli – turvallistamistyypistä.

Tämä tutkimus on kuitenkin saavuttanut tavoitteensa jos sen myötä ymmärrämme yhden tutkimuksen verran enemmän turvallistamisen prosessin mekanismeja.

Niin kuin laadullisessa tutkimuksessa aina, konteksti ratkaisee.

# 6. LÄHDELUETTELO

## PRIMÄÄRIAINEISTO

### Instituutioaineisto:

Suomen kyberturvallisuusstrategia ja taustamuistio (2013), Valtioneuvoston periaatepäätös, Turvallisuuskomitean sihteeristö, Helsinki, 24.1.2013.

Kyberturvallisuusstrategian toimeenpano-ohjelma (2014), Turvallisuuskomitea, Puolustusministeriö, Helsinki 11.3.2014.

Valtioneuvoston puolustusselonteko, Valtioneuvoston kanslian julkaisusarja 5/2017, Valtioneuvoston kanslia, 16.2.2017.

Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi, Raportti, tekijät Martti Lehto, Jarno Limnéll, Eeva Innola, Jouni Pöyhönen, Tarja Rusi, Mirva Salminen, Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017, Valtioneuvoston kanslia, 17.2.2017.

Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017 – 2020 (2017), Turvallisuuskomitea, Puolustusministeriö, Helsinki, 10.4.2017.

”Tiedustelulainsäädännön hankkeet käynnistettiin”, Tiedote, Sisäministeriö, 1.10.2015.

”Siviilitiedustelun ja Suojelupoliisin ohjausta kehitetään”, Uutinen, Sisäministeriö, 10.11.2016.

”Suomi tarvitsee siviilitiedustelua kansallisen turvallisuuden suojaamiseen”, Tiedote, Sisäministeriö, 19.4.2017.

”Tiedustelulaki kirvoitti laajasti lausuntoja, palaute pääosin myönteistä”, Tiedote, Sisäministeriö, 11.7.2017.

”Siviilitiedustelulainsäädäntöä pidetään tarpeellisena ja kannatettavana”, Tiedote, Sisäministeriö, 7.9.2017.

”Siviilitiedustelulaki parantaisi Suomen kansallista turvallisuutta”, Tiedote, Sisäministeriö, 25.1.2018.

”Tiedustelulakikokonaisuus eteni eduskunnan käsiteltäväksi”, Uutinen, Sisäministeriö, 25.1.2018.

”Esitys luottamuksellisen viestin suojaa koskevan perustuslain säännöksen muuttamisesta eduskunnalle”, Tiedote, Oikeusministeriö, 25.1.2018.

”Tiedustelulain tarpeeseen liittyviä käytännön esimerkkejä”, Sisäministeriö, luettu viimeksi 24.6.2018.

”Siviilitiedustelulainsäädäntö - kysymyksiä ja vastauksia”, Sisäministeriö, luettu viimeksi 24.6.2018.

”Hallituksen esitys eduskunnalle laiksi tiedustelutoiminnan valvonnasta ja laiksi valtion virkamieslain 7 §:n muuttamisesta”, Valiokunnan mietintö PeVM 9/2018 vp─ HE 199/2017 vp, Perustuslakivaliokunta.

## Sanomalehtiaineisto:


Andersson, Li (2018), ”Keskustelu tiedustelulaeista on hankalaa siksi, että käsitteitä käytetään tarkoitushakuisesti”. Helsingin Sanomat. 24.2.2018. Mielipide.

Ervasti, Pekka (2015), ”Pekka Ervasti: Laiton lailliseksi” Yle. 26.6.2015. Uutinen.

Grünn, Emma (2017), ”Presidentti Niinistö Turun joukkopuukotuksesta: Viikonlopun aikana terrori tuli Suomeen – "Vain yhdessä selviämme". Yle. 20.8.2017. Uutinen.

Halminen Laura (2017a), Tuomo Pietiläinen ”Salaisuus kallion uumenissa – juuri kukaan ei tiedä, mitä tekee Puolustusvoimien Viestikoekeskus, mutta nyt HS:n saamat asiakirjat avaavat mysteerin”. Helsingin Sanomat. 16.12.2017. Politiikka.

Halminen, Laura (2017b), Tuomo Pietiläinen, Paavo Teittinen ”Suomi pääsee uusien tiedustelu-lakien myötä käsiksi Venäjältä kaapelien kautta tulevaan tietoon – Miten se muuttaisi Suomen ja Yhdys-valtojen suhteita?”. Helsingin Sanomat. 19.12.2017. Politiikka.

Halminen, Laura (2018a), ”Hallitus esittää, että perustuslakia on muutettava kiireellisesti eli jo eduskunnan 5/6-enemmistön päätöksellä.”. Helsingin Sanomat. 20.2.2018. Politiikka.

Halminen, Laura (2018b), ”Kyberpommit” ja ”massaurkinta” ovat uhkapuhetta, joka vie tiedustelulakien ymmärtämistä väärään suuntaan”. Helsingin Sanomat. 21.2.2018. Politiikka.

Happonen, Päivi (2017), ”Kiisteltyyn tiedustelulakiin tulossa tiukennuksia – Yle sai salaiset lakipykälät etukäteen nähtäväksi” Yle. 8.12.2017. Uutinen.

Jaakkola, Johan (2017), "Vakavin uhka mitä historiamme tuntee" – Näin uuden verkkovalvontalain pelätään muuttavan Suomea”. Yle. 21.1.2017. Uutinen.

Junkkari, Marko (2017), ”Sipilän hallitus ajaa tiedustelulakia nopeutetusti voimaan – Rkp:n kanta voi ratkaista asian”. Helsingin Sanomat. 12.4.2017. Politiikka.

Kervinen, Elina (2018a), ”Turvallisuus ja yksityisyys vaakakupissa – HS kokosi tiedustelulain keskeisemmät kysymykset eduskuntakäsittelyn alkaessa”. Helsingin Sanomat. 18.2.2018. Politiikka.

Kervinen, Elina (2018b), Tuomo Pietiläinen ”Uudet lait voivat tulla voimaan jo 2018 lopussa, jos eduskunnan oppositio kannattaa lakien säätämistä kiireellisinä”. Helsingin Sanomat. 25.1.2018. Politiikka.

Koivisto, Matti (2017), ”Presidentti Niinistö tiedustelulain aikataulusta: "Niin pian kuin mahdollista". Yle. 21.4.2017. Uutinen.

Mäntymaa, Eero (2017), ”Terrorismin uhka Suomessa on kohonnut – mitä se tarkoittaa?”. Yle. 14.6.2017. Uutinen.

Niilola, Merja, (2017), ”Tutkijat nihkeinä tiedustelulakien kiireelliselle säätämiselle – "En näe Suomeen kohdistuvaa poikkeuksellista uhkaa tai kriisiä". Yle. 31.7.2017. Uutinen.

Nurmi, Lauri (2017), ”Pääministeriltä kova uutispommi: Juha Sipilä haluaa tiedustelulakien perustuslakimuutoksen läpi kiireellisenä”. Kaleva. 9.4.2017. Uutinen.

Pantsu, Pekka (2017), ”Suojelupoliisi: Suomessa epäillään ensimmäistä kertaa terroritekoa – uhka-arvio säilyy ennallaan”. Yle. 19.8.2017. Uutinen.

Pietiläinen, Tuomo, Teija Sutinen, Niko Vartiainen (2018), ”Eduskunta hyväksyi perustuslain muutoksen kiireellisenä äänin 178–13 – HS kokosi vastaukset viiteen kysymykseen tiedustelu-laeista”. Helsingin Sanomat. 3.10.2018. Politiikka.

Pietiläinen, Tuomo, Teija Sutinen (2018), ” Presidentti Niinistö hyväksyi perustuslain muutoksen, mutta näpäytti eduskuntaa: ”Perustuslaissa säädettyä menettelyä on syytä kirjaimellisesti noudattaa”. Helsingin Sanomat. 5.10.2018. Politiikka.

Schauman, Satu (2017), ”Tiedustelulaki läpi kiireellisenä? Oikeusministeri Antti Häkkänen: Tarkan harkinnan paikka”. Verkkouutiset. 25.5.2017. Uutinen.

Silfverberg, Kalle (2018), ”Oikeusministeri Häkkänen: Tiedustelulait pitää säätää kiireellisesti”. Helsingin Sanomat. 16.1.2018. Politiikka.

STT (2017), ”Risikko: Tiedustelulaki täytyy saada eteenpäin jo tällä hallituskaudella”. Kaleva. 1.3.2017. Uutinen.

STT (2018), ”Asiantuntijat: Turvallisuusseikat voivat oikeuttaa perustuslain muuttamisen kiireellisenä” Yle. 27.2.2018. Uutinen.

”Supo nostaa profiiliaan uhkakuvien yhdistelmällä”. Helsingin Sanomat. 22.3.2018. Pääkirjoitus.

Teittinen, Paavo (2017), ”Tiedustelulakeihin vaaditaan muutoksia: Asiantuntijoiden mielestä lakien vaikutuksia ja turvallisuusuhkien mittaluokkaa arvioitu puutteellisesti”. Helsingin Sanomat. 21.12.2017. Politiikka.

Tolkki, Kristiina (2017), ”Mistä puhutaan, kun puhutaan tiedustelulaista? 7 keskeistä termiä selitettynä”. Yle. 19.4.2017. Uutinen.

Vartiainen, Niko (2018), ”Tiedustelulakien käsittely alkoi – Yksityiselämän suojaa käsittelevä pykälä halutaan hoitaa nopeasti, mutta sote voi syrjäyttää sen”. Helsingin Sanomat. 5.9.2018. Politiikka.

Vartiainen, Niko (2018), ”Perustuslakivaliokunta puoltaa yksimielisesti tiedustelulakien muutosta ja pitää kiireellisenä julistamista mahdollisena”. Helsingin Sanomat. 21.9.2018. Politiikka.

## KIRJALLISUUS JA ARTIKKELIT

Alasuutari, Pertti (2011), Laadullinen Tutkimus 2.0. 4. uud. p. Tampere: Vastapaino.

Balzacq, Thierry (2005), “The Three Faces of Securitization: Political Agency, Audience and Context” European Journal of International Relations, Vol. 11(2): 171–201.

Balzacq, Thierry (2011), Securitization theory: How security problems emerge and dissolve. London: Routledge.

Buzan, Barry (1991), ”New patterns of global security in the twenty-first Century”. International Affairs 67:3, 431-451.

Buzan, Barry, Ole Wæver & Jaap de Wilde (1998), Security: A New Framework for Analysis. Boulder: Lynne Rienner.

Buzan, Barry & Lene Hansen (2009), Evolution of International Security Studies. Cambridge: Cambridge University Press.

Buzan, Barry & Ole Wæver (2009), "Macrosecuritisation and security constellations: reconsidering scale in securitization theory". Review of International Studies. 35:2, 253 – 276.

Burgess, J. Peter (2010), The Routledge handbook of new security studies. London: Routledge.

Choucri, Nazli (2012), Cyberpolitics in international relations. Cambridge, Mass.: MIT Press.

Costigan, Sean. S., & Perry, J. (2012), Cyberspaces and global affairs. Burlington, Vt.: Ashgate.

Dillon, Michael (2013), Deconstructing international politics. London: Routledge.

Eriksson, Johan., & Giacomello, Giampiero (2007), International relations and security in the digital age. London: Routledge.

Fairclough, Norman (2013), Critical Discourse Analysis: The Critical Study of Language. London: Taylor and Francis.

Hansen, Lene & Helen Nissenbaum (2009), "Digital Disaster, Cyber Security, and the Copenhagen School" International Studies Quarterly (2009) 53, 1155–1175.

Harle, Vilho & Kari Laitinen (2004), "Turvallistaminen, sota ja järjestys muuttuvassa kansainvälisessä järjestelmässä". Kosmopolis 2/2004.

Helmbrecht, Udo (2011), EU cyber security and the role of ENISA. The European Union as a security provider, 49-66.

Ingalsuo, Timo., & Paunu, Pasi (2012), Kyberturvallisuus, hyökkäys ja puolustus. Tampere: Tampereen yliopisto.

Jarvis, Darryl. S. L. (2002), International relations and the "third debate": Postmodernism and its critics. Westport (Conn.): Praeger.

Jokinen, Arja (2016), Diskurssianalyysi: Teoriat, Peruskäsitteet Ja Käyttö. Tampere: Vastapaino.

Juntunen, Tapio (2010), "Kamppailu Suomen turvallisuuspolitiikan linjasta ja turvallisuuden merkityksistä 2010 -luvulle tultaessa". Politiikan tutkimuksen laitos. Tampereen yliopisto.

Kantola, Harry & Rantapelkonen, Jari (2013), "Insights into cyberspace, cyber security and cyberwar in the Nordic countries". The fog of cyber defence, 24-36.

Kenkel, Kai Michael & Luisa Cruz Lobato (2015), "Discourses of cyberspace securitization in Brazil and in the United States" Rev. Bras. Polít. Int. 58 (2): 23-43.

Kremer, Jan-Frederik., & Benedikt Müller (2013), Cyberspace and International Relations: Theory, Prospects and Challenges.

Laitinen, Kari (1999), Turvallisuuden todellisuus ja problematiikka: tulkintoja uusista turvallisuuksista kylmän sodan jälkeen. Tampere: Tampereen yliopisto.

Limnéll, Jarno. (2013), "Offensive cyber capabilities are needed because of deterrence". The fog of cyber defence, 200-207.

Limnéll, Jarno., & Klaus Majewski & Mirva Salminen (2014), Kyberturvallisuus. Jyväskylä: Docendo.

McDonald, Matt (2008), "Securitization and the Construction of Security" European Journal of International Relations, Vol. 14(4): 563–587.

Mikail, Elnur. H. (2012), "The theory of postmodernism as a contemporary international relations theory". International Journal of Academic Research, 4(6), 79-82.

Palokangas, Tero. (2013), "Cyberwar: Another revolution in military affairs?" The fog of cyber defence, 146-153.

Vilkka, Hanna (2015), Tutki Ja Kehitä. 4. uud. p. Jyväskylä: PS-kustannus.

Vuori, Juha A. (2004), "Turvallisuudesta uhkantorjuntaan: Käsitteen kääntöpuolen pohdintaa.". Kosmopolis (34)3, 46 – 51.

Vuori, Juha A. (2008), "Illocutionary Logic and Strands of Securitization: Applying the Theory of Securitization to the Study of Non-Democratic Political Orders". European Journal of International Relations, Vol 14, Issue 1, 65 – 99.

Vuori, Juha A. (2016), "Deterring Things With Words: Deterrence as a Speech Act" New Perspectives, Vol.24, No.2/2016.

Välivehmas, Heikki. (2015), Secure Finland: Information on comprehensive security in Finland. Helsinki: Security Committee.

Wæver, Ole (2011), Politics, security, theory. Security Dialogue 42(4-5) 465-480.

Wæver, Ole (2015), The theory act: Responsibility and exactitude as seen from securitization. International Relations 29(1), 121-127.